Connected Vehicle & Services (CV&S)

Product Specifications Document

Phone as a Key (PaaK)

Version 2.2.1

06/16/2020

PRINTED COPIES ARE UNCONTROLLED

FORD MOTOR COMPANY CONFIDENTIAL

The information contained in this document is

Feature Document
PaaK

Proprietary to Ford Motor Company.

Disclosure or distribution to unauthorized persons is strictly prohibited.

Feature Document

PaaK

TABLE OF CONTENTS

CHANGE CONTROL

Table 0 Revision History

Revision	Author	Description	Sections Affected	Release Date
0.1	Praveen Yalavarty / Suvrat Jain	Initial Delivery at 80% Target Date	All	9.19.2016
0.2	Brian Wilkerson / Eugene Karpinsky / Nick Rosa	Post Initial Delivery, realigned and merged initial PSD document (by Suvrat J) with additional content from EESE	All	11.18.2016
0.3	Ziad AlHihi / Eugene Karpinsky	Feature re assessed, Formatted the doc, added more details and few sections, updated use cases, fixed the references, merged some sections and cleaned the doc.	All	12.28.2016
0.4	Ziad AlHihi / Michael Simons / Eugene Karpinsky / Fouad Bounefissa	Updated / Added all Sequence Diagrams.	All	2.13.2017
0.5	Ziad AlHihi	Formatted the document and organized the content in many sections / added the onboard and off board interface diagrams	All	2.15.2017
0.6	Ziad AlHihi / Fouad Bounefissa	Updated functional requirements	10	2.20.2017
0.7	Ziad AlHihi / Victor Gonzalez	Updated and added non-functional requirements	11	2.20.2017
0.8	Ziad AlHihi / Fouad Bounefissa / Victor Gonzalez	Revised many sections in functional and non-functional requirements	10 & 11	2.22.2017
0.9	Ziad AlHihi/	Updated and reviewed all sections	All	2.24.2017
0.9	Brian Wilkerson	Revised functional requirements reformatted some sections.	10 & 11	2.24.2017
0.11	Tricia Tobolski	Updated enrollment section	10.1.3	3.1.2017
0.12	Tricia Tobolski	Update to include removal of all passwords stored in the BLEM from master reset and PaaK feature reset	1.13 and 1.14	3.2.2017
0.13	Tricia Tobolski	Terms and conditions for PaaK are contained in the mobile app terms and conditions.	7.4 use case 3.1 and 3.2	3.3.2017
0.14	Ziad AlHihi	Updated all Use Cases, added titles and revised some sections. Updated TOC.	7.2, 7.3, 7.4	3.6.2017
0.15	Ziad AlHihi	Updated all tables and figures. Revised functional requirements.	10	3.6.2017
0.16	Ziad AlHihi	Updated all onboard and off board sequence diagrams.	9	3.26.2017
0.17	Ziad AlHihi	Updated the Interface Diagram and The State Diagram.	6.4 & 8	3.26.2017
0.18	Ziad AlHihi	Cleaned up the whole documents and updated the TOC.	All	3.26.2017

0.19	Ziad AlHihi	Updated the Acronyms, PaaK System Elements, PaaK State Diagram, all Use Cases & the Appendices.	4.1, 6.2, 6.4, 7, 13	3.28.2017
0.20	Tricia Tobolski	PaaK Reset HMI trigger	10.4.3	3.29.2017
0.21	Tricia Tobolski	Update Subscription Management use case 3.1 steps to shorten.	3.1	3.30.2017
0.22	Ziad AlHihi / Victor Gonzalez	Added use cases to the pre and post conditions, Updated requirements, updated the order of all tables and figures, Revised Sequence Diagrams	7, 9, 10, All	3.30.2017
1.0	Ziad AlHihi	Updated all sections and sequence diagrams.	All	3.31.2017
1.1	Fouad Bounefissa, Ziad AlHihi, Victor Gonzalez	Update per Feedback Sheet PaaK March 31 Spec Drops. See section 11 for details, updated use cases (added revoke key from another device), and updated Subscription Management and Functional requirements.	All	5.5.2017
1.2	Fouad Bounefissa, Ziad AlHihi, Victor Gonzalez	Requirements Update. See section 11 for details	All	6.1.2017
1.3	Fouad Bounefissa, Ziad AlHihi, Victor Gonzalez	Requirements clarification. See section 11 for details	All	6.23.2017
1.4	Fouad Bounefissa, Ziad AlHihi, Victor Gonzalez	Requirements clarification. See section 11 for details	All	9.11.2017
1.4.1	Fouad Bounefissa	Requirements clarification. See section 11 for details	All	04.05.2018
2.0	Fouad Bounefissa	Updated document to include FNV2 specs	All	7.20.2018
	Fouad Bounefissa	Updated Resets specs to prevent MyKey to execute reset functions	All	6.20.2019
2.1	Fouad Bounefissa	Changed connectivity manager to reflect BLEM peripheral mode	All	02.15.2020
2.2.2	Jack Turner	Minor clarifications for FNV3	All	1/10/2022

Commented [JT1]: Is there a later update to the spec to include RePA?
Didn't see anything for Park. RePA, etc, and for example Use Case 2.3 will need modifications.
I think we will also need PRD updates, but didn't see that document in the MY22 GEN2 folder.

Feature Document
PaaK

1 OVERVIEW

1.1 Purpose

This document is intended to capture the features and functions of the Phone-as-a-key (PaaK) feature from a customer standpoint. The document shall be used to define the functional behaviour of the system and components for both on-board and off-board interfaces.

1.2 Scope

PaaK is intended to allow a mobile device to replicate today's fob-based PEPS (Passive Entry Passive Start) and IKT (Integrated keyfob technologies) using BLE (Bluetooth low energy) as a wireless transport.

The following describes the scope delivered for the initial launch of PaaK:

- Markets/Region:
  PaaK shall be launched in U.S., Canada, Mexico, Europe and China
  - Europe shall not support RHD (right hand drive) vehicles
  - LHD (left hand drive) Markets: Austria, Belgium, Switzerland, Denmark, Germany, Spain, France, Italy, Netherlands, Norway, Portugal, Finland, Sweden, Greece, Hungary, Poland, Romania, Czech Republic
- Vehicle/ Programs
  - CGEA1.3C platform:
    - U611 MY20
    - CX483 MY21
    - U554 MY21
  - FNV2 platform:
    - CX727 MY21, MCA MY24
    - P702 BEV MY22
    - U540 MY21
    - MY23 CX483 MCA
  - FNV3 Platform
    - MY23 CDX707
    - MY24 U611 MCA

- PaaK will launch on vehicles starting with Bundle 4
- Mobile App Integration / Customer Facing
  - Request a CAK
  - Pair Phone with BLEM
  - Check CAK status
  - Revoke CAK from Mobile Device
  - Passive key support from the customer's PaaK enabled phone:

        - passive unlock, passive lock, Walk Away Lock, passive start, passive double lock, Welcome lighting, farewell lighting, open sesame, rear cargo area closure open / close, front cargo area closure open / close, passive charge cord unlock
    - RKE (remote key entry) functions using the customer's PaaK enabled phone:
        - lock, unlock all doors, remote start, remote start extend, remote start status, cancel remote start, rear cargo area closure open/close, vehicle chirp (2x press of lock on key fob), front cargo area closure open / close, global windows open & close
    - Allow CRC/FMC360 to check status of a customer's CAK and revoke a specific customer's CAK
    - Perform PaaK Feature Reset to revoke CAK
    - Perform Master Reset to de-authorize the ECG and revoke CAK
- Feature Enablers
    - BLEM Supplier Feed process
    - BLEM Provisioning
    - BLEM, TCU and ECG Replacement
- Vehicle integration of on-board components:
    - BLEM/BLEAM, TCU, ECG, SYNC, SDLC, Cluster, BCM

1.3 Audience

The following table lists all stakeholders, who shall be involved in the creation and maintenance of this SRD. Refer to the Roles & Responsibilities page in the in the Ford RE Wiki for a list of common Ford roles and responsibilities.

Name	**CDSID**	**Role**
John Van Wiemeersch	Jvanwiem	Supervisor – Electrical Arch, Connectivity & Adv Features
Brian Wilkerson	*bwilker1*	*CV&S Product Supervisor, PaaK Feature Owner*
Ziad AlHihi	*Zalhihi*	*PaaK System Integration Engineer*
Jeff Hamel	Jhamel7	Product Line Owner
Koka Phani	pkoka1	PaaK System Integration Engineer
Victor Gonzalez	gvictor8	PaaK System Integration Engineer
Jack Turner	Jturn259	PaaK Product Engineer
Bharath Chandrashekhar	Bmayann1	PaaK Product Engineer
Eugene Karpinsky	Ekarpins	Core Feature Owner & FIP
Zakiya Gaillard	Zmcclend	PaaK System Integration Engineer
Dante Crockett	*Dcrocket*	*Feature Owner Manager*
Abraham Philip	aphilip	Product Group Manager
Ron Brombach	Rbrombac	Supervisor - Body and Security Subsystems
Micheal Nikiforuk	Mnikifor	Supervisor Core Feature Owner & FIP
Vivekanandh Elangovan	velango5	EESE R&A Development Engineer
Laura Hazebrouck	*Lhazebro*	*EESE R&A Development Engineer*
Daniel King	dking13	Senior Engineer - Body and Security Subsystems
Faten Fawaz	Ffawaz	CV&S Basic Design Vehicle Engineer
Kevin Hille	Khille	Technical Specialist - Body and Security Subsystems
Chad Boes	Cboes	PD IT, BA
David McNabb	*dmcnabb5*	*EESE R&A Development Engineer*
Jochen Schubert	Jschub11	IT Cyber Security
Mike Westra	Mwestra	Supervisor - IT Cyber Security
Sergii Rudenko	*srudenk1*	*IT Mobile App Architect*
Nick Davio	Ndavio	I&E Engineer
Kevin Militello	*Kmilitel*	*IT Advanced Product Definition*
Khalil Alward	kalward1	EESE, TCU Engineer

Tim Thivierge	Tthivier	EESE BLEM Core Engineer
Kelly Zechel	Kzechel	Ford Pass Marketplace
Igor Reznick	*Ireznick*	*PaaK FI Integration Manager*
Matheswaran Rackiannan	mrackian	CVPODS Anchor
Steven James Craig	scraig33	PaaK IT Program Manager
Fouad Bounefissa	*Bfouad*	*Solution Architect*
Mike Simons	*msimmo60*	*PaaK System Integration Engineer*

Table 1 Audience

2 REFERENCES

The references with the versions in the table below were used when this document was created. There may be some updates in later versions of these documents and in such case please refer to the original documents.

Document Title	Version	Physical Name / Location
BLEM/BLEAM PaaK SPSS (CGEA)	1.3	BLEM Hardware Specs
BLEM/BLEAM PaaK SPSS (FNV2, 3)	1.3	BLEM Hardware Specs
BLEM Provisioning specs		BLEM Provisionig SPSS
BLEM/BLEAM PaaK Common Function SPSS	1.0	PaaK BLEM/BLEAM PaaK Common Function SPSS
Key Management Specs	0.3	Key Management Specs for PaaK
BLE Module Security Requirements	0.3.0	BLE Interface Security Specification PaaK
Mobile App Security Specs	0.9	Mobile App Security Specifications for PaaK
Security Requirements	0.7	Security Requirements Specs
Security - SYNCP Functional Specification	1.22	SYNCP Functional Specification
Security - SYNCP Services Assignment	1.42	SYNCP Services Assignment
Master Reset	2.0	Master Reset Specific Systems Engineering Spec
App Signing Specs	0.2	App Signing Specs
BCM Requirements		FS-MU5T-14B476-ACA
Supplier Feed Specification	0.1	Supplier Feed Specification
TCU SPSS	1.0	APIM Infotainment Subsystem Part Specific Specification (SPSS)
CVFMA Requirements	3.0	CVFMA PRD
BSP PRD	2.7	BSP Requirement Specification
ECG Spec		TBD

Table 2 References

3 ACRONYMS & NOTATION

3.1 Acronyms

BCM	Body Control Module
BLEAM	Bluetooth Low Energy Antenna Module. It allows to utilize smart phone for traditional fob purposes like remote operation (remote start, luck/unlock, etc), passive entry, passive charge code unlock and passive start.
BLEM	Bluetooth Low Energy Module (BLE). Module responsible for providing the BLE interface for the vehicle.
BLEM supplier feed	A data feed from the BLEM supplier providing key metadata about the BLE module to the vehicle data store GVMS.
BLEM Replacement	A dealer activity to replace a malfunctioning BLE Module. Separate follow-on processes will need to address data update and synchronization with the SDN and additional tasks – Target ID Transfer key exchange with the BCM
BSP	Backup Starting Passcode. Allows customers to enter and drive away their fob-based PEPS-class vehicle without their PEPS fob or PaaK key. This feature utilizes the existing keypad entry system as well as a new, password-based starting system. Intended only as a backup feature.
CAK	Consumer Access Key, the secure keys that are stored in the BLEM and Mobile Device
Central Lock	Locking feature disables exterior door handles from operating when lock button is pressed
Charge Cord	Charging cord are used to charge HEVs, BEVs and PHEVs at charging ports. Charge cord ports can be locked to prevent theft.
CVBOP	Connected Vehicle Business Operations Portal Provides Operations Support and CRC representatives with direct access to key states per VIN. CRC can also revoke keys on behalf of customer that phone in if their mobile device was lost or stolen and they desire to remove access for the specific Phone.
CVFMA	Connected Vehicle Feature Management Application
CVFTA	Connected Vehicle Ford Telematics Application (FT FI)
Double Lock	Locking feature disables both the exterior and interior door handles from operating when lock is pressed twice within 3 seconds on the key fob. Turning the ignition on or electronically unlocking the vehicle (except via Power Door Lock switches), will un-double lock the vehicle. Thatcham Requirement. Europe Markets only
EOL	End of Line
FNV2	Fully Networked Vehicle 2 An advanced in-vehicle networked architecture intended to succeed the current CGEA 1.3c architecture. FNV2 provides enhanced in-vehicle computing, speed and information based architecture capability to deliver improved user experiences and enterprise features faster to production and over the entire life cycle of the vehicle. System architecture built around the ECG (Enhanced Central Gateway)
FNV3	Fully Networked Vehicle 3 The FNV3 architecture is being developed in order to expand SOA to body systems. The FNV3 Body Systems Project is the next step in the evolution of Ford vehicle electrical systems into a Services Oriented Architecture (SOA).
HS1_RFA	Remote Function Actuator (Netcom). Also see BLEM.
IPC	Instrument Panel Cluster
Intelligent Access Key, PEPS Key / Fob	Customer keyfob.
IVSS	In-vehicle Security Services. IVSS will be leveraged to generate the keys to be delivered to the mobile device and vehicle BLEM

Lincoln Way / Ford Pass App	Mobile App for Lincoln or Ford vehicles. Key changes to be made to Lincoln App and Ford Pass to support PaaK feature requirements, both customer UI and for key exchange and pairing functionality
Lincoln Embrace	Activate welcome lighting in Lincoln vehicles
PaaK	Phone as a Key is a connected vehicle feature that leverages a virtual key stored in the customer's mobile device and a Bluetooth Low Energy Module in the vehicle to deliver certain CV functions
PEPS	Passive Entry- Passive Start
TCU	Telematics Control Unit. The TCU module is the gateway between the on-board client, BLEM and the PaaK Off Board Client, New Generation Service Delivery Network (SDN) to provide secure communication.
Welcome Mode	Welcome Mode will illuminate select exterior lighting when the PaaK mobile device enters within 3m radius of the vehicle.
System	System refers to the overall eco-system from the cloud to the vehicle
MyKey	MyKey is a restricted driving mode setting that promotes good habits, such as increasing seat belt use, limiting vehicle top speeds and decreasing audio volume.
Enhanced Memory	Enhanced Memory adds to driver identification and recall of user profile that typically include positional settings as well as radio presets, climate control settings, navigation preferences.
GVMS	Global Vehicle Management System is a component in the cloud that stores BLEM ESN/VIN relationship (or GVMS)
Component	A minimal eco item (e.g. ECU) that can be tested in isolation.
User	An individual or group that benefits from a system during its utilization.
Actor	A role played by a person who interacts with the subject of development.
Validation	A confirmation, through objective evidence, that the requirements for a specific intended use or application have been fulfilled.
SDN	This is an infrastructure by which Connected Services and Solutions are transmitted and received from the Vehicle for processing (includes Connected Vehicle Feature Management Application, system administrator, vehicle and marketing)
GVMS	Global In Vehicle Information System
RVCM	Remote Vehicle Configuration Manager
HS1_CAN	High Speed 1 Controller Area Network (CAN)
HS3_CAN	High Speed 3 Controller Area Network (CAN)
HS4_CAN	High Speed 4 Controller Area Network (CAN)
FD1_CAN	Flexible Data Controller Area Network 1
FD2_CAN	Flexible Data Controller Area Network 2
LIN	Local Interconnect Network
SSP	Subscription Services Platform
SuMO	Subscription Management
VCS	Vehicle Configuration Server
GAP	Bluetooth Generic Access Profile
GATT	Bluetooth Generic Attribute Profile

Table 3 Acronyms & Notations

3.2 Notation

3.2.1 Requirements Templates

Each requirement (including goals and use cases) in the document shall start with the following heading, which gives a unique ID and a Title, followed by a description of the requirement (see below).

The heading shall be formatted by using the header styles “RE_Requirement”. The requirement ID shall be prefixed and suffixed with 3 hash characters. This will ease the import to VSEM (refer to "How to import specifications into VSEM as separate requirements") and enables indexing.

###<Req ID>### <Title>

<Description>

The guideline “How to write better requirements” shows how to structure the textual description of a requirement.

3.2.2 Identification of Requirements

The unique requirement ID given in the headline of the requirement follows the requirement throughout the development process. The requirement ID format follows a well-defined syntax.

All identifiers in a document shall be composed of 4 parts:

- A leading prefix, which indicates the type of requirement (R=Requirement, UC=Use Case, SC=Scenario, …)
- A prefix, which indicates the abstraction level (F=Feature, FNC=Function, CMP = component).
- Followed by a name, indicating the scope, which the requirement belongs to (e.g. feature or function name)
- Ending with the actual requirement number

Example:

R_FNC_LockArbitrator_00004	This is the fourth requirement on function level for the function Lock Arbitrator.

4 ASSUMPTIONS, CONSTRAINTS AND DEPENDENCIES

4.1 Assumptions

An assumption provides information about the availability, performance, or skills required to deliver the feature. The assumptions for this feature are:

- BLEAM does not have a supplier feed
- Packaging of the BLEM and BLEAMs shall not inhibit the user experience.
- BLEM is able to launch the mobile app with no user interaction using iBeacon technology

4.2 Dependencies

A task dependency is a relationship between two tasks in which one task depends on another to begin. Dependencies can be created between two or more tasks, tasks and tasks groups or between two or more task groups. The dependencies for this feature are:

- Vehicle must be equipped with bundle 4 TCU or bundle 5 PHEV TCU and ECG or greater
- BCM must support PEPS, Remote Start, Passive Start/Entry, Welcome Mode, Passive Charge Cord Unlock, Frunk unlock, Enhanced Memory and MyKey for these features to work
- Vehicle must support Windows Global Open & Global close for those features to be presented in the mobile app and function
- Vehicle must contain BLEM, BLEAMs and associated technology
- Feature capability must be resolvable in CVFMA at the ECU component level
- Mobile App components must be supported on Lincoln Way and Ford Pass Mobile App
- PaaK capable Mobile devices must support Bluetooth 4.2 or later

- Authentication capability of the mobile device and BLEM
- PaaK will use existing functionality for adding a VIN to the mobile app
- PaaK will use common feature management constructs including CVFMA and VCS, and Subscription Management functionality for enrollment and activation as needed
- Subscription Management will utilize auto subscribe process Vehicle must be equipped with a backup keyless entry system, BSP (Backup Starting Passcode)
- Vehicle must be equipped with valet mode, BSP (Lincoln Backup Ignition)
- Vehicle connectivity is required for CRC CAK revoke

4.3 Constraints

A constraint is any project limitation that could impact the schedule, budget, performance, and overall result. The constraints for this feature are:

- Independent BLE antennas instead of leveraging fob-based PEPS antennas.
- As Antennas Array may vay by vehicle type or market region, the performance of the system may be impacted. Refer to Vehicle Specs table in Apendix section of this document.
- Phone localization and Inside/outside detection algorithm used to locate mobile device
- The solution will utilize in vehicle hardware modules/design constructs as determined for PaaK – BLEM/BLEAM modules.
- Key delivery process requires backend systems with a high availability.
- CAK revoke through TCU is not possible when the vehicle is in deep sleep

The following table describe the difference between the ECG equiped vehicle and the FNV2 equipped Vehicle

Paa*K* FEATURE & MARKET SCOPE SUMMARY

Content	PaaK Bundle 4	PaaK Bundle 5
Vehicle Programs	U611 MY20(Lead)	CX727 MY21
Markets	U.S.A , Canada and China, Mexico	U.S.A, Canada, China, LHD Europe
Key Fob	2 Key Fobs, 4 Door PEPS, 360 Approach Lighting	1 KeyFob, Passive Start Only
BLE Modules / Antennae's	1 BLEM, 10-11 BLE Antennae's(program specific)	1 BLEM, 7 BLE Antennae's
Mobile App	Lincoln Way Mobile App	Ford Pass Mobile App
PaaK Customer Facing	Up to 4 PaaK devices / Phone Keys	Up to 4 PaaK devices / Phone Keys
	4 Door PEPS 360 Approach Lighting	2 Door PEPS Side Approach Lighting
	RKE (lock, unlock, panic), remote start, lift gate access	RKE (lock, unlock, panic), remote start, lift gate access, frunk, Charge Cord Unlock
	Enhanced Memory Support	Enhanced Memory Support
PaaK Backup/Guest Mode	PaaK Backup Start Passcode – code entry & start; Enhanced Valet Mode – temp auto-generated code	PaaK Backup Start Passcode – code entry(7 digits for EU) & start; Enhanced Valet Mode – temp auto-generated code

Bold *represents new/revised*

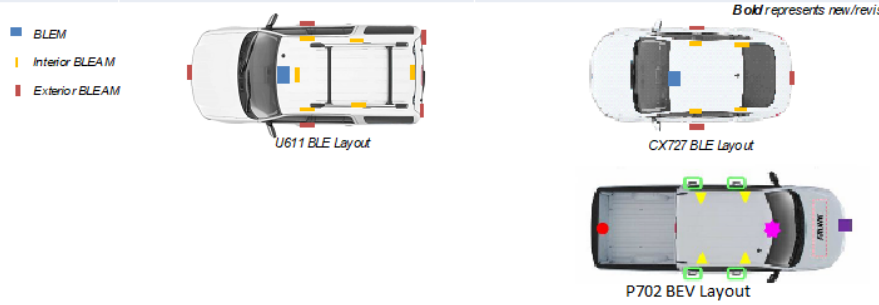


Figure 1 PaaK Features & Market Scope

5 FEATURE OVERVIEW

Phone-as-a-key (PaaK) is a feature that duplicates Fob-based Passive Entry Passive Start (PEPS) functionality with traditional key fob keys. It enables the use of a customers registered and authorized connected mobile device to deliver the features provided by the keyfob. PaaK passive & active features will be activated when a customer's mobile device is detected within a predefined radius by the BLEM/BLEAM subsystem.

5.1 Feature Function / Element List

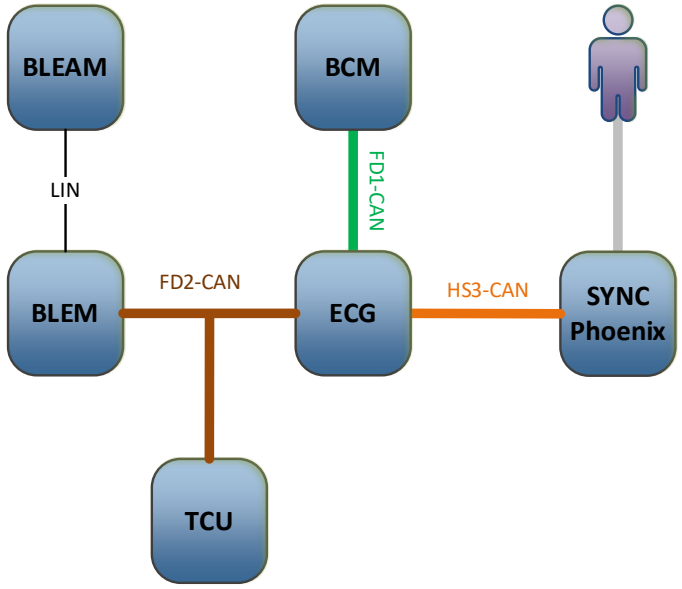


Figure 2.1 ECG FNV3 Architecture Diagram

Feature Document
PaaK

			PaaK System Components				
			On Board				
	Functions	Description	BLEM	BLEAM	BCM	ECG	APIM_CDC
PaaK Active Commands	Unlock	User issues unlock command via mobile app	✓		✓	✓	
	Lock	user issues lock command via mobile app	✓		✓	✓	
	Remote Start	User issues remote start command via mobile app	✓		✓	✓	
	Remote Start Extend	User issues extend remote start command via mobile app	✓		✓	✓	
	Remote Start Cancel	User issues remote start cancel command via mobile app	✓		✓	✓	
	Remote Start Status	Remote start status displayed to user via mobile app	✓		✓	✓	
	Operate Front Cargo Area	User issues front cargo area closure release / open / close command via mobile app	✓		✓	✓	
	Panic	Use issues panic command via mobile app	✓		✓	✓	
	Windows Up	User issues windows up command via mobile app	✓		✓	✓	
	Windows Down	User issues windows down command via mobile app	✓		✓	✓	
	Operate Rear Cargo Area	User issues rear cargo area closure release / open / close command via mobile app	✓		✓	✓	
PaaK Passive Functions	Welcome Mode / Approach Detection	Smartphone provides response to vehicle when device is in Welcome Mode rande	✓		✓	✓	
	Farewell Mode	Smartphone provides response to vehicle when device enters Farewell Mode range	✓		✓	✓	
	Passive Lock	User touches exterior unlock switch on vehicle closure	✓		✓	✓	
	Passive Unlock	User touches exterior lock switch on vehicle closure	✓		✓	✓	
	Walk-Away Lock	Smartphone provides response to vehicle when user enters Walk Away Lock range	✓		✓	✓	
	Open Sesame	User waves foot through rear closure sensor area to operate rear cargo closure	✓		✓	✓	
	Passive Start	User applies brake and presses start button	✓		✓	✓	

Table 4 FNV3 Onboard System Elements

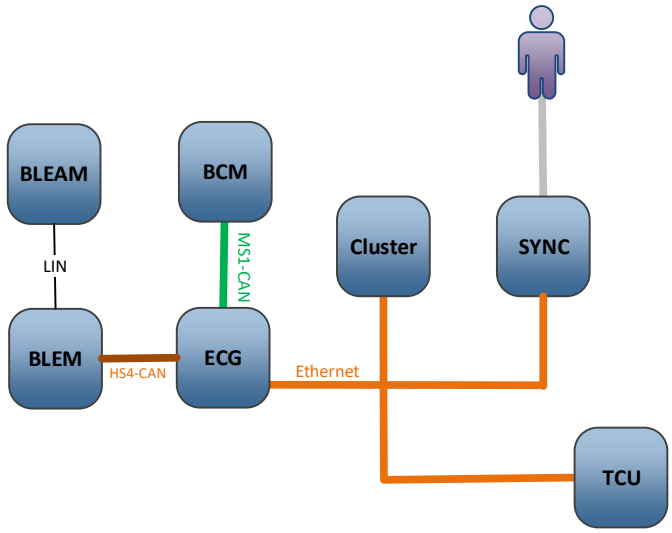


Figure 2 ECG Architecture diagram

Feature Document

PaaK

			PaaK System Elements					
			On-Board					
	Options	Description	BLEM	BLEAM	BCM	ECG	APIM	IPC
PaaK Active Commands	Unlock - Driver	User issues Unlock command via Mobile App						
	Lock	User issues Lock command via Mobile App	✓		✓	✓		
	Remote Start	User issues Remote Start command via Mobile App	✓		✓	✓		
	Extend Remote Start	User issues Extend Remote command via Mobile App	✓		✓	✓		
	Remote Start Cancel	User issues Remote Start Cancel command via Mobile App	✓		✓	✓		
	Remote Start Status	Remote Start Status displayed to user via Mobile App	✓		✓	✓		
	Panic	User issues Panic command via Mobile App	✓		✓	✓		
	Unlock Frunk	User issues Unlock command via Mobile App	✓		✓	✓		
	Vehicle Chirp	User issues Vehicle Chirp command via Mobile App	✓		✓	✓		
PaaK Passive	Welcome Mode/Approach Detection	Smartphone provides input to Welcome Mode feature once device is in Welcome Mode Range	✓		✓	✓		
	Farewell Mode	Smartphone exits Farewell Mode range	✓		✓	✓		
	Passive Unlock	User pulls exterior door handle	✓		✓	✓		
	Passive Lock	User presses exterior switch on door handle	✓		✓	✓		
	Open Sesame	User waves leg through Open Sesame sensor	✓		✓	✓		
	Charge Cord Unlock	User pressesCharge Cord door	✓		✓	✓		
	Lift Gate / Lid Release	User presses button on rear handle or lift gate	✓		✓	✓		
	Passive Start	User applies brake and presses push-to-start button	✓		✓	✓		

Table 5.1 FNV2 Onboard system elements

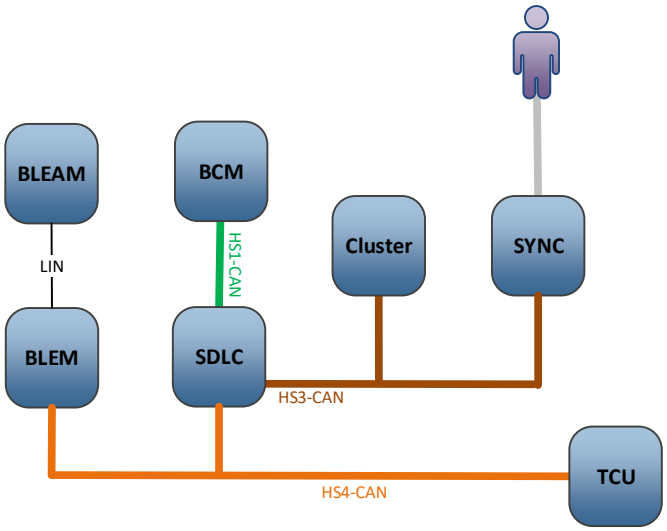


Figure 3 CGEA Architecture diaram

			PaaK System Elements					
			On-Board					
	Options	Description	BLEM	BLEAM	BCM	SDLC	APIM	IPC
PaaK Active Commands	Unlock - Driver	User issues Unlock command via Mobile App						
	Lock	User issues Lock command via Mobile App	✓		✓	✓		
	Remote Start	User issues Remote Start command via Mobile App	✓		✓	✓		
	Extend Remote Start	User issues Extend Remote command via Mobile App	✓		✓	✓		
	Remote Start Cancel	User issues Remote Start Cancel command via Mobile App	✓		✓	✓		
	Remote Start Status	Remote Start Status displayed to user via Mobile App	✓		✓	✓		
	Panic	User issues Panic command via Mobile App	✓		✓	✓		
	Vehicle Chirp	User issues Vehicle Chirp command via Mobile App	✓		✓	✓		
PaaK Passive	Welcome Mode/Approach Detection	Smartphone provides input to Welcome Mode feature once device is in Welcome Mode Range	✓		✓	✓		
	Farewell Mode	Smartphone exits Farewell Mode range	✓		✓	✓		
	Passive Unlock	User pulls exterior door handle	✓		✓	✓		
	Passive Lock	User presses exterior switch on door handle	✓		✓	✓		
	Open Sesame	User waves leg through Open Sesame sensor	✓		✓	✓		
	Lift Gate / Lid Release	User presses button on rear handle or lift gate	✓		✓	✓		
	Passive Start	User applies brake and presses push-to-start button	✓		✓	✓		

Table 6 CGEA Onboard system elements

	Options	Description	PaaK System Elements											
			Off-Board											
			SDN	Mobile App	Mobile Device	CVFMA	PaaK FI	Supplier	CRC / CVBOP	GVMS	Subscription Management	IVSS Core	IVSS Cloud	GiVIS
Platform / Support	BLEM 4.2 Support	BLEM implementation based on Bluetooth 4.2 Specification Standard			✓									
	BLE Consumer Device Support	iOS or Android Smartphones with Bluetooth 4.2 or above to be supported			✓									
	Single Smartphone / Multiple Vehicles	PaaK enabled on multiple vehicles with one device	✓	✓	✓		✓	✓						
	Multiple Smartphones / Multiple Vehicles	PaaK enabled on multiple vehicles with multiple devices	✓	✓	✓		✓							
Pre-Enrollment / Verification	Supplier Feed	BLEM supplier data feed with metadata about the module to GiVIS						✓		✓		✓		✓
	Vehicle Capability Check	User triggers Capability Check via Mobile app HMI once Mobile app registered and VIN specified	✓	✓		✓					✓			
	Provisioning	Provisioning request once BLEM & TCU installed in vehicle	✓							✓			✓	✓
	Self-Test / Diagnostics	Special process initiated via Diagnostic testing or once the new VIN is received by BLEM												
Enrollment / De-Enrollment	Request CAK	User initiates PaaK key via Mobile App	✓	✓			✓						✓	
	Generate CAK	Back-end functionality to generate key pair/CAK	✓	✓			✓						✓	
	Deliver CAK	Process to deliver the CAK into the Vehicle/Mobile App	✓	✓										
	Track CAK State	Back-end functionality to track CAK state	✓	✓			✓		✓					
	Revoke CAK	User initiates PaaK key revoke via Mobile App	✓	✓			✓		✓					
	Master Reset	User performs Master Reset procedure from SYNC	✓			✓	✓				✓			

Table 7 PaaK System Elements

5.2 Context Diagram

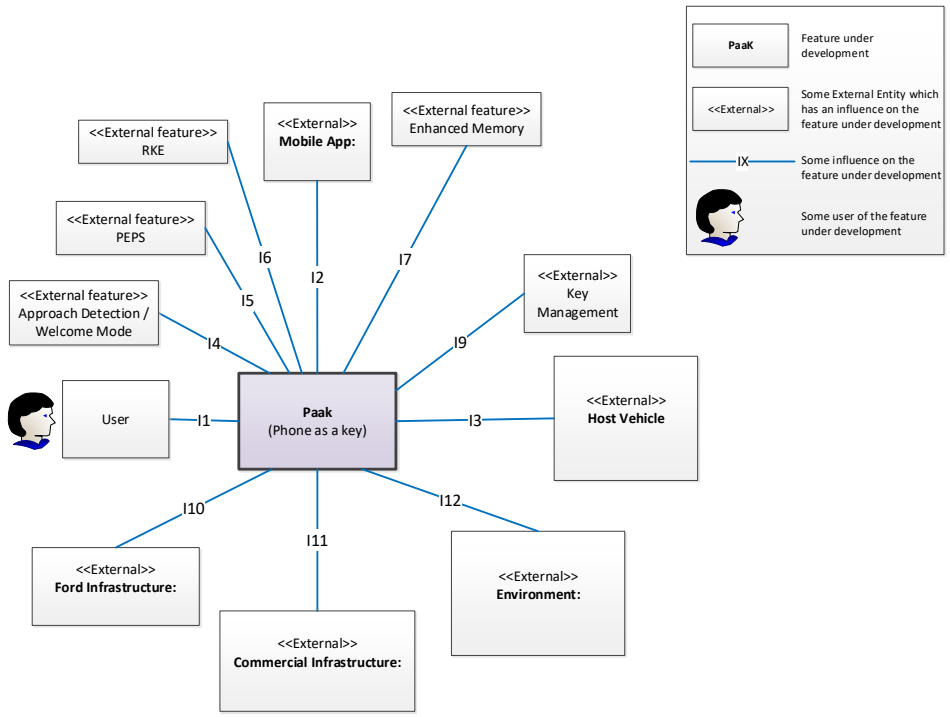


Figure 4 PaaK Context Diagram

Interface ID	Interaction	Influence	Influence Description
I1	Users with PaaK enabled mobile device	Approach Vehicle; Unlock/Lock Vehicle; Open/Close Door; Service	User Request is used as an input to trigger feature functions based on phone location (Approach detected / Welcome Mode enabled , etc.); also used for servicing needs
I2	Mobile App via API	Vehicle functionality via Mobile App	User Request to initiate Remote Start (Remote Start / No Request); User Request to Unlock/Lock a vehicle (/ Unlock All Doors / Lock All Doors / / No request); User Request to open vehicle liftgate (Open / No Request)
I3	Host Vehicle	Provides input of the following states: Ignition State Vehicle Speed Lock State Engine State	Current state of vehicle Ignition (Off / Acc / Delayed Acc / On); Vehicle Speed (>= 8KPH); Vehicle Locks (Locked Double / Locked All / Unlocked All / Unlocked Driver/Walk away Lock); Engine State (Engine Not Running / Engine Running)
I4	Welcome Mode feature	Search Request/ Search Result	Used as input to Welcome Mode Request for phone location (Request phone location / No request) and as an output Response to Welcome Mode Search Request (Phone in approach Zone / Phone not in Approach Zone)

I7	Enhanced Memory feature	User Profile ID	Provides output and allows Enhanced Memory feature to identify user phone to recall its associated Driver profile
	MyKey	Key Type	Provides output and allows MyKey feature to determine whether the phone has MyKey access restrictions (MyKey / Not MyKey)
I9	Key Management	Add / Revoke Vehicle and Phone Certificates	Allows provision of a new certificate to the vehicle & phone; Revokes an existing certificate from a phone & vehicle
I5	Passive Entry function	Search Request / Search Result	Passive Entry Request for phone location (Request Phone Location / No Request) and provides output Response to Passive Entry Search Request (Phone in Entry Zone / Phone Not in Entry Zone)
	Pre-Authorization	Search Request/ Search Result	Used as input to Pre-authorization for phone location (Request phone location / No request) and as an output Response to Pre Authorization Mode Search Request (Phone in passive entry Zone / Phone not in passive entry Zone)
	Walk Away Lock	Search Request/ Search Result	Used as input to Walk Away Lock for phone location (Request phone location / No request) and as an output Response to Walk Away Lock Mode Search Request (Phone in Approach Detection Zone / Phone not in Approach Detection Zone)
	Passive double lock	Search Request / Search Result	Passive double Lock Request for phone location (Request Phone Location / No Request) and provides output Response to Double Lock Search Request (Phone in Entry Zone / Phone Not in Entry Zone)
	Passive Charge Cord Unlock	Search Request / Search Result	Passive Charge Cord Unlock Request for phone location (Request Phone Location / No Request) and provides output Response to Passive Charge Cord Unlock Search Request (Phone in Entry Zone / Phone Not in Entry Zone)
	Passive Start function	Search Request / Search Result	Passive Start Request for phone location (Request Phone Location / No Request) and provides output Response to Passive Start Search Request (Phone in Start Zone / Phone Not in Start Zone)
I6	Remote Keyless Entry	Unlock / Lock Request	User Request to Unlock or Lock vehicle (Unlock All Doors / Lock All Doors / No Request)
	Remote Keyless Entry	Panic Request	User Request to enable vehicle Panic Alarm (Panic / No Request)
	Remote Keyless Entry	Liftgate Request	User Request to Open vehicle liftgate (Open / No Request)
	Remote Keyless Entry	Frunk Unlock	User Request to enable Frunk Unlock
	Remote Start	Remote Start Request	User Request to initiate vehicle Remote Start (Remote Start / No Request)
	Extend Remote Start	Remote Start Request	User Request to extend vehicle Remote Start (Remote Start / No Request)
I12	Environment	External Environment	External environmental effects such as Temperature differentials (influence to external/internal antennas for phone location calculation); EMC/ESD effects (consumer devices with LF/UHF, Bluetooth, Radio towers, Wi-Fi, etc.); RF barriers (buildings, vehicles); fluid ingress (spill on antennas); ice/snow ingress; Dust/Mud
I10	Ford Infrastructure: Ford Assembly Plants / Service	EOL / Light test / Module Replacement	System affects due to module replacement / manufacturing processes
I11	Commercial Infrastructure: Back Office	Interaction between On-Board and Off-Board via Cellular	Input/output collaboration with Cloud-Vehicle interface

	Structure / SDN		

Table 8 Feature Influences

5.3 Feature Modes and States

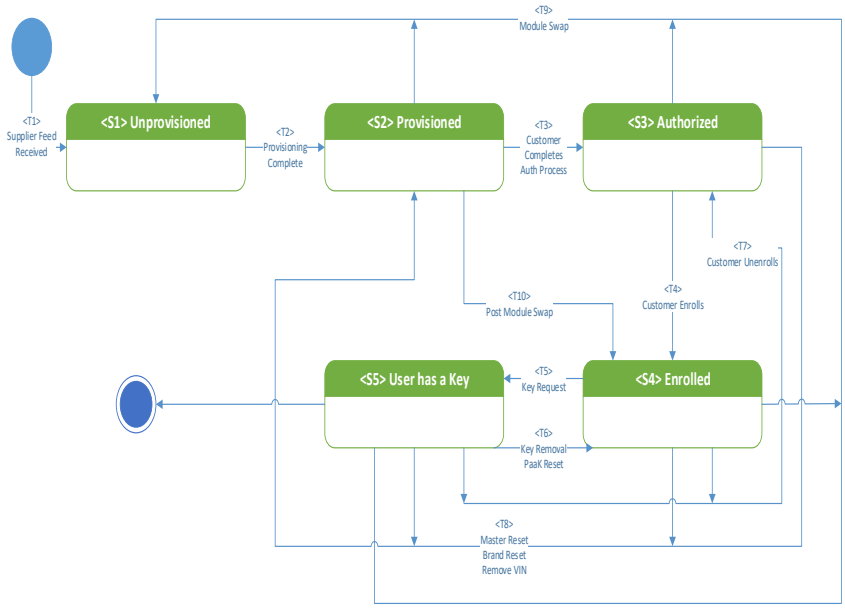


Diagram 1 PaaK State Diagram

State ID	Name	Description
<S1>	Unprovisioned	The BLEM and TCU/ECG are not provisioned in this state
<S2>	Provisioned	The BLEM and TCU/ECG are provisioned by associating them in the cloud in this state
<S3>	Authorized	The vehicle and customer are associated using the existing authorization process in this state
<S4>	Enrolled and Subscribed	Auto subscribe process completed per TCU/ECG Authorization process (automated process) which results in free PaaK subscription and enrollment in CVFMA

<S5>	User has a key	This state is reached when the user has a valid CAK on their phone and in their vehicle. All PaaK Active and Passive functions are performed within this state.

Table 9 Operational states

Transition ID	Name	Description
<T1>	Supplier Feed Received	Supplier feed is received by Ford
<T2>	Provisioning Complete	This transition occurs when the BLEM module has completed the provisioning process
<T3>	Customer Completes Authorization Process	This transition occurs when the customer has agreed to the in-vehicle authorization popup and the authorization status is updated in SDN.
<T4>	Auto Subscribe	Upon TCU/ECG authorization, the customer is automatically subscribed and enrolled in PaaK per Auto Subscribe process.
<T5>	Key Request	The customer requested a key and the key has been stored in their phone and vehicle
<T6>	Key Removal	The customer performs a key revoke, PaaK reset or uninstalls their app the key will be removed
<T7>	Customer Un enrolls	This transition occurs when the customer un enrolls and unsubscribes from PaaK
<T8>	Master Reset, Brand Reset or Remove VIN	This transition occurs when the customer performs a master reset or removes the VIN in the mobile app
<T9>	Module Replacement	The BLEM module is replaced in the vehicle
<T10>	Post Module Replacement	After the new BLEM module is installed. There is no need to re-authorize or re-enroll and subscribe.

Table 10 Transition between Operational States

6 System Use Cases

6.1 System Component / Actors

Actor	Description
User	User with mobile device (smartphone) (with intent of accessing and/or driving a vehicle)
Cluster	digital instrument panel instrumentation that displays gauges and other important information for the customer
Mobile Device	Smartphone belonging to user with the Mobile App installed
Mobile App	Mobile Application installed on the User's Mobile Device
BLEM Manufacturer	Provides supplier feed
BLEM	Bluetooth Low Energy Module
Vehicle Manufacturer	Ford Co.
Vehicle	Active vehicle that the user is attempting to access
EOL	End of Line configuration process
Dealer	User to support customer's initial set up of PaaK feature
Service Technician	User responsible for post-customer delivery services (performing module replacement and other required services)
SDN	This is an infrastructure by which Connected Services and Solutions are transmitted and received from the Vehicle for processing (includes Connected Vehicle Feature Management Application, system administrator, vehicle and marketing)
GiVIS	Global In Vehicle Information System
IVSS	In Vehicle Security Service is a software system used to control software security for vehicle critical modules.
GEC Hub	Drop point for Supplier data. TCU manufacturer sends encrypted TCU feed file GECHub mailbox
GVMS	Global Vehicle Management System is a component in the cloud that stores BLEM ESN/VIN relationship
BCM	Body Control Module is responsible for controlling electronic accessories in the vehicle's body
APIM	Also known as SYNC is the vehicle's HMI
PaaK FI / CVPODS	Is a connected vehicle feature that leverages a virtual key stored in the customer's mobile device and a BLEM in the vehicle to deliver certain CV functions
CVBOP	Connected Vehicle Business Operations Portal, used for feature package creation
CVFMA	Connected Vehicle Feature Management Application: Provides a common, generic – data driven set of constructs, evaluates vehicle capability on specified triggers
Vehicle Profile	Receives information about vehicle capability published from CVFMA (as defined in Feature Packages in CVBOP) and stores vehicle capability
xAPI	Retrieves information about vehicle capability as stored in Vehicle Profile and exposes it to the mobile app

Table 11 System Component Actors

6.2 Use Cases Table

Use Case Table	
Vehicle Use Cases	
ID	Name
1.1	Initial Pairing with Key Delivery
1.2	Supplier Feed
1.3	BLEM Provisioning
1.4	Phone BLE Connection Termination
1.5	Mobile Device Location Detection
1.6	Passive Commands
1.7	Master Reset
1.8	PaaK Reset
1.9	BLEM / BLEAM Self-Test
1.10	Enhanced Memory Association / Disassociation
SDN Use Cases	
ID	Name
2.1	Auto-Subscription
2.2	Key State Check – CRC
2.3	CAK Revoke - CRC
Mobile App Use Cases	
ID	Name
3.1	Capability Check - Mobile Device
3.2	CAK Request
3.3	Remove Vehicle
3.4	CAK Revoke – Same Mobile Device
3.5	Key State Check – Mobile Device
3.6	Active Commands
3.7	Secondary User Authorization
3.8	CAK Revoke - Different Mobile Device

Table 12 Use case table

6.3 Use Cases Diagram

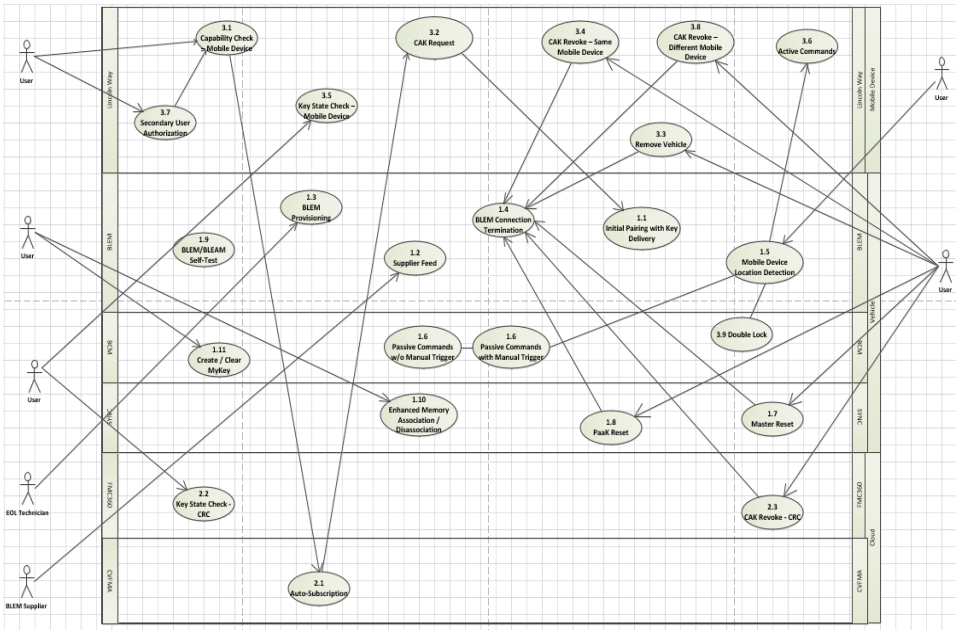


Diagram 2 PaaK Use Case Diagram

For more details, check the Use Case Diagram in SharePoint. *For organizational purposes, user was expanded into different sections of the use cases.

6.4 Vehicle Use Cases

UC 1.1 Initial Pairing with Key Delivery

Use Case ID	1.1
Use Case Name	**Initial Pairing with Key Delivery**
Description	User delivers the CAK to the BLEM and initial pairing process follows

Normal Flow	1- BLEM iBeacon and BLE constantly advertising when TCU/ECG is authorized 2- Upon key request and installation in the mobile device the user moves close to vehicle with the mobile app in the foreground 3- The mobile app scans for selected vehicle's Beacon 4- The Phone detects the advertising, recognizes the Beacon ID and initiates a connection with the BLEM 5- The BLEM initiates a soft authentication by providing a random Counter 6- the Phone responds with a Soft Authentication response by hashing the BLEM UUID concatenated with the provided counter 7- BLEM verifies the SoftAuth response and initiate a BPEK challenge to authorize de mobile device 8- The phone initiates a key delivery and specify the number of SyncP payload to deliver 9- The BLEM request one payload at a time, execute and respond back with success or failure message. 10- BLEM confirms delivery 11- The mobile notifies PaaK FI via the SDN that CAK was delivered successfully. The notification shall be queued if mobile device could not connect to the cloud. The Vehicle will also notify the cloud via TCU about successful key delivery
Actor (s)	Mobile device, BLEM
Pre-condition(s)	User request CAK from cloud CAKs are generated and delivered to the mobile device
Triggers	User physically approach the vehicle to start connection
Post Conditions	BLEM CAK is delivered to the vehicle Active / Passive commands are available
Exceptions	1. User does not have physical access to his vehicle 2. Connection is interrupted by customer (i.e. walking out of the BLE range) *Please refer to PaaK System DFMEA for further details on possible exceptions 3. Server Message I is out of sequence (OOS) *Refer to Paak SPSS for OOS scenarios

UC 1.2 Supplier Feed

Use Case ID	**1.2**
Use Case	**Supplier Feed**
Description	Supplier Feed provides BLEM metadata into GVMS.
Normal Flow	1. The supplier feed metadata is sent to GEC Hub. 2. IVSS reads the feed and updates GVMS. 3. GVMS processes and publishes the Supplier feed metadata to GVMS. 4. Supplier shall be notified prior for their part shipment via GEC Hub.
Actor (s)	BLEM Supplier
Pre-condition(s)	BLEM built OEM Feed delivered to the supplier (reverse supplier feed)
Triggers	BLEM Supplier provides Supplier feed metadata to Ford GEC Hub.
Post Conditions	BLEM supplier metadata is available in GVMS/IVSS.
Exceptions	1. Metadata not uploaded to GVMS/IVSS 2. GVMS/IVSS fail to either publish the feed metadata or publish a response back to the supplier. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.3 BLEM Provisioning

Use Case ID	**1.3**
Use Case Name	**BLEM Provisioning**
Description	The process when the ECG (FNV2, 3) or /TCU (CGEA) exchanges BLEM's ESN through TCU with regional service delivery network (SDN) for offline data validation/verification.
Normal Flow	1. Installing of the BLEM & TCU/ECG in the vehicle and recognizing each other. 2. The BLEM will send an ESN and additional hardware/software data provisioning request Via TCU. Get a provisioning acknowledgment alert to BLEM via TCU. 3. BLEM Provisioning information is sent to GVMS 4. GVMS stores BLEM ESN/VIN relationship. 5. Offline BLEM data validation process on GVMS 6. PaaK FI is notified
Actor (s)	BLEM, SDN, GVMS
Pre-condition(s)	• ECG and/or TCU provisioning completed, • Target ID Transfer process between BLEM, BCM completed, • BLEM Supplier feed already ingested in GVMS, • The BLEM DID status checked in manufacturing plant to ensure it is in un-provisioned state. • Service routine to initiate provisioning is performed successfully
Triggers	BLEM installed in vehicle and TargetID is learned and locked.
Post Conditions	1. BLEM goes into provisioned state
Exceptions	1. The BLEM fails to send provisioning request. 2. The ECG (FNV2, 3) or TCU(CGEA) fails to submit the provisioning request to the SDN. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.4 Phone BLE Connection Termination

Use Case ID	**1.4**
Use Case Name	**Phone BLE Connection Termination**
Description	If the Mobile Device has initiated the connection termination, mobile device must trigger a BLE session termination to the BLEM.
Normal Flow	1. User initiates a connection termination (i.e. device is turned off, key revoke, PaaK Reset) 2. Mobile Device terminates BLE session with BLEM 3. BLEM will not report this device to BCM 4. No key detected appears on the Cluster
Actor (s)	BLEM, BCM, Mobile App
Pre-condition(s)	1. Mobile device and vehicle BLEM have consumer access keys (CAK) stored. 2. Mobile Device and BLEM initially paired. 3. BLEM has completed and succeeded in Bluetooth Module Mobile Device Validation. 4. CAK Revoke – Mobile Device Use Case 5. Remove Vehicle Use Case 6. Master Reset, Brand Reset and PaaK Reset Use Cases

Commented [JT2]: Impact to this process to include RePA capability?

Triggers	1. A CAK revoke process is initiated from either mobile app or vehicle (PaaK Reset / Master Reset) 2. Mobile Device exits detection ranges of BLEM. *Please refer to PaaK System DFMEA for further details on possible exceptions
Post Conditions	Connection between the BLEM and mobile device is terminated.
Exceptions	1. Mobile device fails to initiate the Connection Termination. 2. BLEM is not responding. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.4 Phone BLE Connection removal

Use Case ID	**1.4**
Use Case Name	**Phone BLE Connection removal**
Description	If the Mobile Device has initiated the connection removal, BLEM must initiate a Re-pairing request to the mobile device to recreate the paring configuration.
Normal Flow	1. User initiates a connection removal (i.e. deviBLE connection is deleted from Bleutooth settings) 2. Mobile Device terminates BLE session with BLEM 3. BLEM will re-pair with the mobile device
Actor (s)	BLEM, BCM, Mobile App
Pre-condition(s)	1. Mobile device and vehicle BLEM have consumer access keys (CAK) stored. 2. Mobile Device and BLEM initially paired. 3. BLEM has completed and succeeded in Bluetooth Module Mobile Device Validation.
Triggers	1. User deletes bleutooth configueration from his device (forget bleutooth connection). *Please refer to PaaK System DFMEA for further details on possible exceptions
Post Conditions	Connection between the BLEM and mobile device is recreated.
Exceptions	1. Mobile device fails to initiate the Connection Termination. 2. BLEM is not responding. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.5 Mobile Device Location Detection

Use Case ID	**1.5**
Use Case Name	**Mobile Device Location Detection**
Description	BLEM scans for Mobile device via Bluetooth Low Energy.

Normal Flow	1. Phone and vehicle establish a secure connection 2. BLEM sends a challenge request to Mobile device via Bluetooth Low Energy when in the localization zone, mobile device responds with a challenge response. 3. BLEM calculates the Mobile device location with respect to vehicle using appropriate algorithm.
Actor (s)	Mobile App, BLEM.
Pre-condition(s)	1. Mobile device is in Bluetooth range with the car and connected. 2. Mobile device and vehicle BLEM have consumer access keys (CAK) stored.
Triggers	Mobile Device enters Vehicle localizationzone (6 m).
Post Conditions	1. BLEM has calculated the approximate location of the Mobile Device and can respond to the BCM with a zone location of the mobile device. 2. Active and Passive Commands Use Cases Follow
Exceptions	1. Cannot calculate the Mobile Device location 2. Device is not detected *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.6 Passive Commands with manual Trigger

Use Case ID	**1.6**
Use Case Name	**Passive Commands**
Description	The process of triggering a passive command after Mobile Device localization in an appropriate zone around and inside the vehicle.
Normal Flow	1. BLEM and Mobile Device are in communication range and have successfully paired in Bluetooth Module Mobile Device Validation. 2. Mobile device location has been determined in the appropriate zone with respect to the vehicle. 3. User triggers a passive function by interacting with the vehicle (i.e. user grabs the door handle, push the Start button) 4. The BCM completes the passive function (i.e. unlocks the door).
Actor (s)	User, Mobile App, BLEM, BCM
Pre-condition(s)	1. Mobile device and vehicle BLEM have consumer access keys (CAK) stored. 2. Mobile Device and BLEM are connected 3. BLEM is successfully able to maintain Location Detection (Location Detection Use Case).
Triggers	User triggers a passive function by interacting with the vehicle.
Post Conditions	BCM triggers a search signal to the BLEM to provide key indexest of detected authorized devices for the specified zone
Exceptions	1. Mobile device not able to maintain BLE communication with BLEM. 2. BLEM not able to determine location of the authorized Mobile device. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.6 Passive Commands without Trigger

Use Case ID	**1.6**
Use Case Name	**Passive Commands**
Description	The process of triggering a passive command by localizing Mobile Device in an appropriate zone around the vehicle.

Normal Flow	5. BLEM and Mobile Device are in communication range and have successfully paired in Bluetooth Module Mobile Device Validation. 6. Mobile device location has been determined in the appropriate zone with respect to the vehicle. 7. The BLEM report device location to BCM for passive command execution (Welcome light, Charge Cord unlock, walk away lock) 8. The BCM completes the passive function.
Actor (s)	User, Mobile App, BLEM, BCM
Pre-condition(s)	4. Mobile device and vehicle BLEM have consumer access keys (CAK) stored. 5. Mobile Device and BLEM are connected 6. BLEM is successfully able to maintain Location Detection (Location Detection Use Case).
Triggers	Mobile device localization in trigger zone.
Post Conditions	BLEM triggers a command request to BCM for the specified zone.
Exceptions	3. Mobile device not able to maintain BLE communication with BLEM. 4. BLEM not able to determine location of the authorized Mobile device. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.7 Master Reset

Use Case ID	**1.7**
Use Case Name	**Master Reset (Super Reset)**
Description	User initiates a Master reset procedure from the SYNC HMI to clear all vehicle settings.
Normal Flow	1. The customer Initiates Master Reset via SYNC HMI. 2. A first popup will be displayed for Master Reset warning the customer that their keys will be deleted. 3. Customer clicks continue on the first popup, a second popup will be displayed informing the customer that the keys are going to be deleted and prompt the customer if he wants to continue. 4. BLEM receives the Master reset signal over CAN and ECG (FNV2, 3) or TCU(CGEA) sends Master Reset request to Vehicle SDN and the ECG or TCU is de-authorized. 5. CVFMA de-enrolls VIN in PaaK and subscription cancellation status is updated in the Subscription Management. 6. PaaK FI sends a revoke request to the Mobile App via the cloud 7. Mobile App revokes CAK, and all previously authorized users are notified about a Master Reset event.
Actor (s)	BLEM, SYNC, SDN, ECG (FNV2, 3), TCU
Pre-condition(s)	1. SYNC System is not in Valet Mode. 2. The ignition status signal is equal to “RUN” 3. CAK key is not configured as a MyKey
Triggers	User triggers a Master Reset procedure from the SYNC HMI.
Post Conditions	1. The CAKs in the BLEM are deleted all BSP codes/all passwords on the BLEM are deleted 2. Mobile Devices CAKs are deleted. 3. User is de-authorized and un-subscribed to PaaK. 4. BLE Connection Termination Use Cases follows

Exceptions	1. Inability to access to user settings memory, reset operation is not performed. 2. TCU failed to clear the user settings and change the authorization status. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.8 PaaK Reset

Use Case ID	**1.8**
Use Case Name	**PaaK Reset**
Description	User initiates a PaaK reset procedure from the SYNC HMI to clear all keys.
1. Normal Flow	1. User is inside of the vehicle. 2. User accesses settings and initiates a PaaK Reset procedure from the SYNC HMI. 3. BLEM receives the PaaK reset signal over CAN and sends request to Vehicle SDN via TCU and the ECG (FNV2, 3) or TCU (CGEA) is still authorized. 4. PaaK FI sends a revoke request to the Mobile App via the cloud
Actor (s)	BLEM, SYNC, SDN, ECG (FNV2, 3), TCU.
Pre-condition(s)	1. SYNC detects appropriate signal from the BLEM and displays the PaaK reset menu. 2. Sync System is not in Valet Mode 3. Ignition status signal is equal to "RUN" 4. CAK key is not configured as a MyKey
Triggers	User triggers a PaaK Reset procedure from within the vehicle SYNC HMI.
Post Conditions	1. CAK in the BLEM is deleted, all BSP codes/all passwords on the BLEM are deleted 2. Mobile Device CAK is deleted 3. User remains authorized and subscribed to PaaK 4. BLEM Connection Termination Use Case follows
Exceptions	1. Inability to access to user settings memory, reset operation is not performed. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.9 BLEM / BLEAM Self-Test

Use Case ID	**1.9**
Use Case Name	**BLEM / BLEAM Self-Test**
Description	Antenna self-test initiated to identify the BLEM / BLEAM at different locations of the vehicle
Normal Flow	1. Trigger the test with a diagnostic testing request. BLEM obtains new Vehicle Identification Number (VIN) via CAN. 2. Antennas self-test initiated to identify the Bluetooth Low Energy Antenna Modules at different locations of the vehicle. 3. Each identified BLEAM gets an ID assigned to it from the BLEM 4. BLEM performs a test to validate it as a transmitter and the BLEAM as a receiver. 5. BLEM perform a test to validate it as a receiver and the BLEAM as a transmitter.
Actor (s)	BLEM, BLEAM
Pre-condition(s)	BLEM & BLEAM correctly installed in the desired vehicle.
Triggers	Tester initiates this use case via Diagnostics Testing or once the new VIN is received by BLEM

Commented [JT3]: Does this now remove keys that also have RePA entitlements?

Post Conditions	BLEM is aware of the current state of all BLEAMs.
Exceptions	1. ID can't be assigned to BLEAMs (DTC is set for not identifiable BLEAMs). 2. BLEM can't be validated as a transmitter (DTC is set). 3. BLEM can't be validated as a receiver (DTC is set) *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.10 Enhanced Memory Association / Disassociation

Use Case ID	**1.10**
Use Case Name	**Enhanced Memory Association / Disassociation**
Description	The user performs mobile device associations/disassociations with the driver profile.
Normal Flow	1. The User enters the Driver profile HMI setting menu. 2. User chooses to create/edit Driver profile. 3. User selects to associate/disassociate a Mobile device to that profile. 4. User presses the lock button to confirm association/disassociation.
Actor (s)	User, BLEM, SYNC, Mobile App
Pre-condition(s)	1. Enhanced Memory User Profile Feature set to ON. 2. Mobile device and vehicle BLEM have active consumer access keys (CAKs). 3. Mobile Device is inside the vehicle. 4. Ignition Status is Run.
Triggers	The User decided to create/edit Driver Profile and associate/disassociate the Mobile device to it via SYNC HMI Interface.
Post Conditions	The chosen Mobile device is now associated/disassociated to the active Driver Profile.
Exceptions	1. Mobile App not able to communicate with vehicle via BLE. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 1.11 Create / Clear MyKey

Use Case ID	**1.11**
Use Case Name	**Create / Clear MyKey**
Description	The user Creates/ Clears MyKey Phone.
Normal Flow	1. While inside the vehicle, User selects the Sync Menu Settings → MyKey → Create MyKey Phone. 2. Using Mobile App GUI of the Mobile Device to be programmed as MyKey, the user sends RKE Unlock or Lock command. 3. A popup "Key restricted at next start. Label this Key" shall be seen. 4. To clear MyKey settings User selects the Sync Menu Settings → MyKey → Clear MyKey Phone. 5. The BLEM sends a message to the backend to update the key status (set/unset MyKey)
Actor (s)	User, BLEM, BCM, IPC, Mobile App

Pre-condition(s)	1. MyKey Feature set to ON. 2. Mobile device and vehicle BLEM have active consumer access keys (CAKs). 3. Mobile Device and BLEM paired and connected; Mobile Device is inside the Vehicle. 4. Ignition Status is Run. 5. Have the Administrator Key or PaaK Mobile Device inside the car.
Triggers	The User decided to create/clear MyKey association via IPC settings menu.
Post Conditions	The chosen Mobile device is now created/cleared as MyKey device.
Exceptions	1. Mobile App not able to communicate with vehicle via BLE. 2. Mobile App crashes.

6.5 SDN Use Cases

UC 2.1 Auto-Subscription

Use Case ID	**2.1**
Use Case Name	**Auto-Subscription**
Description	User navigates through mobile app GUI, selects the option and adds VIN.
Normal Flow	1. User navigates to the vehicle details screen and adds VIN 2. Mobile app calls SuMo to perform validate subscription check to determine if user is subscribed to PaaK. 3. SuMo returns response to the mobile app. 4. Mobile app displays option for key request.
Actor (s)	Mobile App, SDN, SuMo, User.
Pre-condition(s)	1. Vehicle is equipped with PaaK capabilities 2. User has downloaded mobile app in his device
Triggers	When user navigates to the vehicle details screen Mobile App HMI triggers a check PaaK Subscription request to determine if user is auto subscribed to PaaK so it knows whether or not to display the key request option to the user.
Post Conditions	1. Auto subscribe process has successfully completed for user per ECG authorization. 2. Mobile app updates HMI to display PaaK options for key request.
Exceptions	1. Call to SuMo fails. 2. Mobile app crashes. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 2.2 Key Status Check - CRC

Use Case ID	**2.2**
Use Case Name	**Key Status Check – CRC**
Description	The call center will be able to check the key status when a customer calls.

Normal Flow	1. Call Center receives call from a customer who has enrolled in Phone-as-a-key. 2. CRC authenticates the user's identity 3. Call Center will first request for the current Key State via CVBOP interfacing to PaaK FI.
Actor (s)	User, CRC.
Pre-condition(s)	Customer has added a VIN to his Lincoln Way/Ford Pass app
Triggers	Customer makes call to Call Center for support.
Post Conditions	Key State from PaaK FI is exposed to FMC360
Exceptions	1. The customer did not provide the right authentication credentials. 2. Call Center did not request for the current Key State. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 2.3 CAK Revoke - CRC

Use Case ID	**2.3**
Use Case Name	**CAK Revoke – CRC**
Description	Consumer Access Key (CAK) can be revoked by placing a call to the Call Center.
Normal Flow	1. Call Center receives call from a customer to delete key in PaaK. 2. Call center confirms the identity of the customer and sends a revoke request to SDN. 3. PaaK FI receives a request from SDN to update the Key state and generate a Delete Consumer Access Key request. 4. BLEM receives a Consumer Access Key (CAK) revoke request from the ECG and provides a revoke confirmation back to the cloud through ECG. 5. SDN initiates a revoke command towards the mobile device
Actor (s)	User, CRC.
Pre-condition(s)	Call Center Check Key State details that Consumer Access Key is in the following state: • Consumer Access Key Ready
Triggers	Customer makes call to Call Center to delete key.
Post Conditions	1. Key State from PaaK FI is updates to CVBOP, Delete the key from the cloud to certain Mobile Device. 2. BLEM Connection Termination Use Case follows
Exceptions	1. The customer did not provide the right authentication credentials. *Please refer to PaaK System DFMEA for further details on possible exceptions

Commented [JT4]: This use case would need to be updated to incorporate RePA entitlement?

6.6 Mobile Device Use Cases

UC 3.1 Capability Check – Mobile Device

Use Case ID	**3.1**
Use Case Name	**Capability Check – Mobile Device**
Description	Once the user downloads the app, the app checks if the device is PaaK compliant.

Commented [JT5]: Does the RePA feature have any communication with this process if, for example the user is enrolled in RePA but their phone does not support it, or does PaaK need to supply messaging?

Normal Flow	1. Mobile app checks if the Mobile device supports BLE 4.2 or greater, and approved mobile device operating system versions. 2. User enrolls in PaaK.
Actor (s)	User, Mobile App.
Pre-condition(s)	1. Mobile App is installed on a Mobile device.
Triggers	Prior to requesting consumer access key.
Post Conditions	1. Capability Check 2. Display Key Request option–
Exceptions	1. Mobile app installation fails *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 3.2 CAK Request

Use Case ID	**3.2**
Use Case Name	**CAK Request**
Description	User utilizes mobile app to request consumer access key from the cloud.
Normal Flow	1. User request CAK via the Mobile App. 2. Mobile App sends CAK request to Vehicle SDN. 3. PaaK FI will validate max key number not reached to a specific VIN. 4. IVSS generates key pair 5. Generated key pair is delivered to PaaK FI and then to Mobile App via SDN.
Actor (s)	User, Mobile App, SDN.
Pre-condition(s)	1. Mobile App shall be installed and the customer created a user account 2. The Vehicle is authorized by at least one user before a CAK can be requested. 3. User has a VIN that is PaaK capable added to his account 4. Device capabilities check is performed for PaaK feature compatibility. 5. The mobile device has internet coverage (connectivity to the cloud) to allow a CAK request.
Triggers	User has requested Key on Mobile App.
Post Conditions	1. User received CAK payload to his Mobile Device in real time from SDN. 2. Initial pairing with key delivery Use Case follows
Exceptions	1. IVSS fails to generate the proper key pair. 2. The generated key pair is not delivered back to PaaK FI by IVSS 3. 4 Keys threshold met. *Please refer to PaaK System DFMEA for further details on possible exceptions

Commented [JT6]: RePA impact?

UC 3.3 Remove Vehicle

Use Case ID	**3.3**
Use Case Name	**Remove Vehicle**
Description	User uses mobile app to remove VIN from their account.

Normal Flow	1. A user removes the VIN from their account using the mobile app 2. And phone revokes key for that VIN from internal memory 3. SDN de-authorizes the user and clears the settings. 4. CVFMA de-enrolls the user from PaaK. 5. Subscription removed for that unique VIN if last user is removed 6. Key revoke sent by PaaK FI and sends it to both BLEM and other customer's devices with the same account. 7. SDN de-authorizes ECG (FNV2, 3) or TCU (CGEA) if last user is removed
Actor (s)	User, Mobile App, SDN.
Pre-condition(s)	User has VIN added to his account
Triggers	User has requested to remove the VIN on Mobile App.
Post Conditions	1. CAK is being removed from BLEM and Mobile Devices 2. BLE Connection Termination Use Case follows
Exceptions	1. User fail to remove the VIN from the account. 2. PaaK FI revoke fails to initiate CAK revoke. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 3.4 CAK Revoke – Same Mobile Device

Use Case ID	**3.4**
Use Case Name	**CAK Revoke – Same Mobile Device**
Description	User sends request to revoke CAK from the same Mobile Device that has the key.
Normal Flow	1. User requests to Revoke Key via Mobile App. 2. Key is deleted locally from the device 3. Mobile App makes a request to PaaK FI via SDN to request a revoke key. 4. PaaK FI receives a call from SDN to update the Key state and generate a Delete Consumer Access Key request. 5. BLEM receives a Consumer Access Key (CAK) revoke request from the cloud through TCU and provides a revoke confirmation back to the cloud through TCU.
Actor (s)	User, Mobile App, SDN.
Pre-condition(s)	Mobile App has Consumer Access Key stored.
Triggers	User has requested Key revoke on Mobile App.
Post Conditions	1. CAK removed from both BLEM and phone 2. BLE Connection Termination Use Case follows 3. If revoked key was a MyKey, the backend sends a notification to the admin users
Exceptions	1. Mobile App fails to delete CAK in internal memory. 2. BLEM fails to delete CAK from internal memory. 3. BLEM does not respond to deletion request. 4. PaaK FI did not receive a call from SDN to update the Key state. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 3.5 Key State Check – Mobile Device

Commented [JT7]: RePA impact?

Use Case ID	**3.5**
Use Case Name	**Key State Check – Mobile Device**
Description	Mobile App will track and display the Key State upon customer's request
Normal Flow	1. User launches the Mobile App. 2. User selects Key State option from Mobile App. 3. Mobile app will display all active keys for the selected vehicle 4. PaaK FI will make updates based on internal key status
Actor (s)	SDN, Mobile App, User.
Pre-condition(s)	Key state Request is sent to the SDN.
Triggers	Customer requests to view the key state.
Post Conditions	Mobile app displays the current key state.
Exceptions	1. Key State cannot be displayed in Mobile app. 2. PaaK FI does not provide the right parameter state. *Please refer to PaaK System DFMEA for further details on possible exceptions

Commented [JT8]: RePA Impact

UC 3.6 Active Commands

Use Case ID	**3.6**
Use Case Name	**Active Commands**
Description	The process to allow the user to perform remote commands via Mobile App
Normal Flow	1. User opens the Mobile App. 2. Mobile App GUI displays possible commands. 3. User taps an icon and triggers an active function such as lock, unlock, frunk unlock, trunk unlock, Windows open, etc. 4. The Mobile App communicates with the BLEM. 5. BLEM communicates with the BCM to complete the commanded active function. 6. Mobile App indicates that the requested active function succeeds.
Actor (s)	User, Mobile App, BLEM.
Pre-condition(s)	1. Mobile device and vehicle BLEM have consumer access keys (CAK) stored. 2. Mobile Device and BLEM initially paired. 3. BLEM has completed and succeeded in Bluetooth Module Mobile Device Validation. 4. Mobile Device Location Detection Use Case
Triggers	User requests an active function via the Mobile App.
Post Conditions	The command is executed by the vehicle. The vehicle state matches the commanded state from the Mobile App for all commands except windows open/close and panic.
Exceptions	1. Mobile App not able to communicate with vehicle via BLE. 2. Vehicle not able to perform the commanded function. *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 3.7 Secondary User Authorization

Use Case ID	**3.7**
Use Case Name	**Secondary User Authorization**
Description	A secondary user is any user that is authorized for a vehicle equipped with PaaK after a primary user has previously been authorized. Vehicle and Mobile CAKs are requested and downloaded by the mobile app for a secondary user
Normal Flow	1. Secondary user requests authorization from the primary user 2. Request is granted and the secondary user hast the option to request CAK 3. CAK request use case from 2. To 5. will follow *Alternative: Secondary user requests a CAK from a different device. Steps 3 to 4 follow.
Actor (s)	Secondary Device, SDN
Pre-condition(s)	1. A secondary user downloads the LW app 2.
Triggers	Secondary user adding the vehicle then requesting CAK from his device.
Post Conditions	1. Secondary user is able to perform all PaaK functionalities 2. Once authorized, secondary user will be able to grant access to more secondary users 3. Capability Check – Mobile Device Use Case follows
Exceptions	1. Secondary user fails to request CAK from mobile app 2. PaaK reached a max of 4 keys and a 5th secondary user requests a CAK 3. Secondary user requesting a key from a different device from their same account 4. Secondary user logs into another device that is not BLE 4.2 capable *Please refer to PaaK System DFMEA for further details on possible exceptions

UC 3.8 CAK Revoke – Different Mobile Device

Use Case ID	**3.8**
Use Case Name	**CAK Revoke – Different Mobile Device**
Description	User sends request to revoke CAK from the different Mobile Device.
Normal Flow	1. Mobile App will present the option to request new key or revoke previous one. 2. User selects to revoke a key presented in another device 3. Mobile App makes a request to PaaK FI via SDN to request a revoke key. 4. PaaK FI receives a call from SDN to update the Key state and generate a Delete Consumer Access Key request. 5. BLEM receives a Consumer Access Key (CAK) Deletion request from the cloud through TCU and provides a delete confirmation back to the cloud through TCU.
Actor (s)	Secondary Device, SDN, BLEM
Pre-condition(s)	Mobile App has Consumer Access Key stored in different device.
Triggers	User has requested Key revoke on Mobile App.

Post Conditions	1. Mobile App deletes CAK and BLEM deletes Consumer Access Key in internal memory for specified key and responds over CAN to status of request. 2. BLEM Connection Termination Use Case follows 3. If revoked key was a MyKey, the backend sends a notification to the admin users
Exceptions	1. Mobile App fails to delete CAK from the internal memory of the other device. 2. TCU is in Deep Sleep mode. 3. Mobile Device or Vehicle is out of coverage area. 4. BLEM fails to delete CAK from internal memory. 5. BLEM does not respond to deletion request. *Please refer to PaaK System DFMEA for further details on possible exceptions

7 SYSTEM INTERFACE

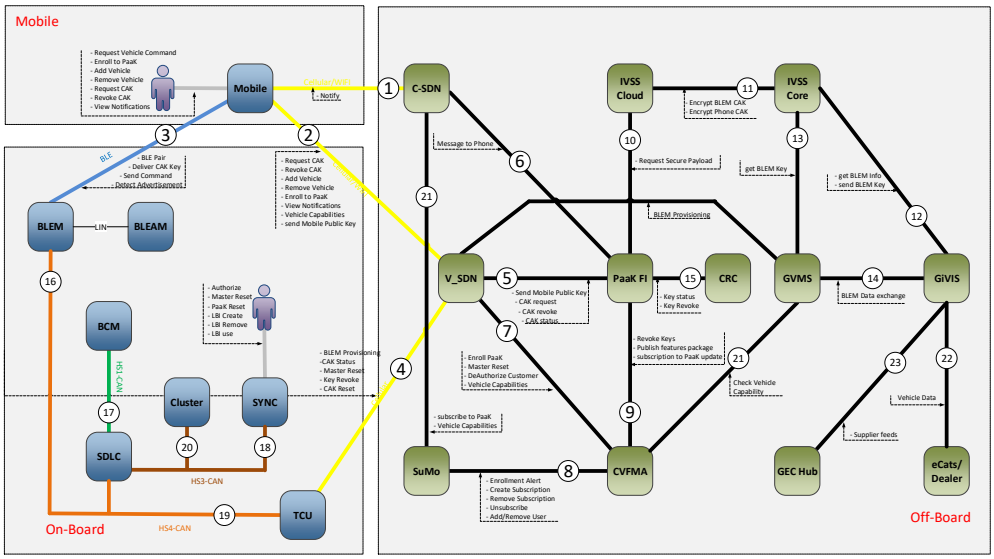


Figure 5 CGEA PaaK Interface Diagram

Interface ID	Descriptions	Parameters / Data structure
1	Communication between Mobile Device and Common SDN	HTTP(S) via Cellular/WIFI
2	Communication between Mobile Device and Vehicle SDN	HTTP(S) via Cellular/WIFI
3	Communication between Mobile Device and the BLEM	RF via BLE
4	Communication Vehicle SDN and TCU	FTCP via Cellular
5	Communication PaaK FI and Vehicle SDN	HTTP(S)
6	Communication between PaaK FI and Common SDN	HTTP(S)
7	Communication between CVFMA and Vehicle SDN	HTTP(S)
8	Communication between CVFMA and Subscription Management	HTTP(S)
9	Communication between CVFMA and PaaK FI	HTTP(S)
10	Communication between IVSS Cloud and PaaK FI	HTTP(S
11	Communication between IVSS Cloud and IVSS Core	HTTP(S
12	Communication between IVSS Core and GVMS	HTTP(S)
13	Communication between IVSS Core and GVMS	HTTP(S)
14	Communication between GiVIS and GVMS	HTTP(S)
15	Communication between CRC and PaaK FI	HTTP(S)
16	Communication between BLEM and ECG	Multiplex packet exchange via CAN (HS4_CAN – SDLC)
17	Communication between BCM and ECG	Multiplex packet exchange via CAN (MS1_CAN)
18	Communication between SYNC and ECG	Ethernet
19	Communication between TCU and ECG	Ethernet
20	Communication between Cluster and ECG	Ethernet
21	Communication between CVFMA and GVMS	HTTP(S)
22	Communication between eCats/Dealer and GiVIS	FTP/HTTP(S)
23	Communication between GecHub and GiVIS	FTP/HTTP(S)

Table 13 PaaK Interfaces Descriptions (CGEA)

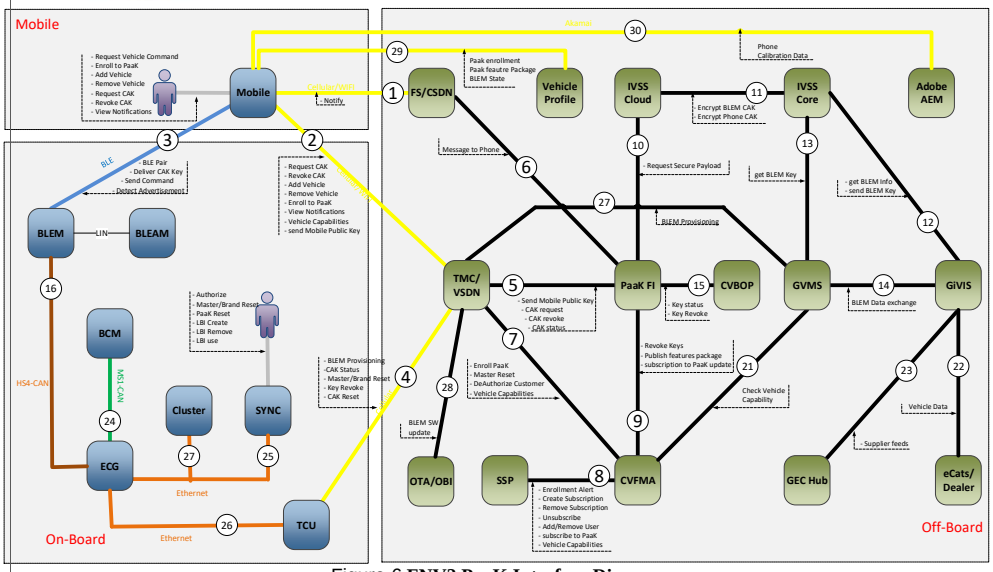


Figure 6 **FNV2 PaaK Interface Diagram**

Interface ID	Descriptions	Parameters / Data structure
1	Communication between Mobile Device and Common SDN	HTTP(S) via Cellular/WIFI
2	Communication between Mobile Device and Vehicle SDN	HTTP(S) via Cellular/WIFI
3	Communication between Mobile Device and the BLEM	RF via BLE
4	Communication between Vehicle SDN and TCU	FTCP via Cellular
5	Communication between PaaK FI and Vehicle SDN	HTTP(S)
6	Communication between PaaK FI and Common SDN	HTTP(S)
7	Communication between CVFMA and Vehicle SDN	HTTP(S)
8	Communication between CVFMA and Subscription Management	HTTP(S)
9	Communication between CVFMA and PaaK FI	HTTP(S)
10	Communication between IVSS Cloud and PaaK FI	HTTP(S
11	Communication between IVSS Cloud and IVSS Core	HTTP(S
12	Communication between IVSS Core and GVMS	HTTP(S)
13	Communication between IVSS Core and GVMS	HTTP(S)
14	Communication between GiVIS and GVMS	HTTP(S)
15	Communication between CRC and PaaK FI	HTTP(S)
16	Communication between BLEM and ECG	Multiplex packet exchange via CAN (HS4_CAN – SDLC)
24	Communication between BCM and ECG	Multiplex packet exchange via CAN (MS1_CAN)
25	Communication between SYNC and ECG	Ethernet
26	Communication between TCU and ECG	Ethernet
27	Communication between Cluster and ECG	Ethernet
21	Communication between CVFMA and GVMS	HTTP(S)
22	Communication between eCats/Dealer and GiVIS	FTP/HTTP(S)
23	Communication between GecHub and GiVIS	FTP/HTTP(S)
27	Communication between V-SDN and GVMS	HTTP(S)

Table 14 PaaK Interfaces Descriptions (FNV2)

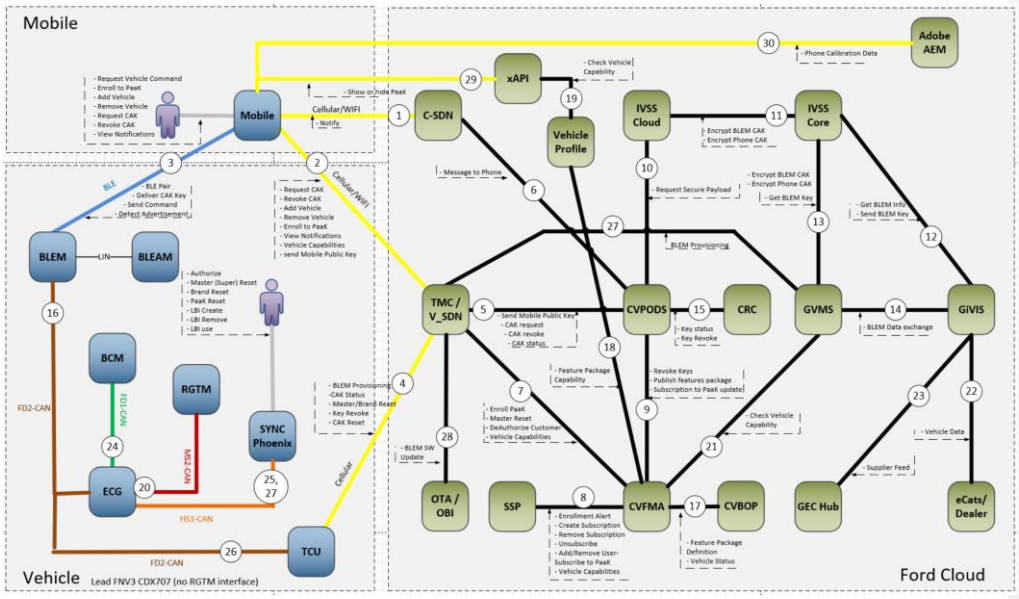


Figure 6.2 FNV3 PaaK Interface Diagram

Interface ID	Descriptions	Parameters / Data structure
1	Communication between Mobile Device and Common SDN	HTTP(S) via Cellular/WIFI
2	Communication between Mobile Device and Vehicle SDN	HTTP(S) via Cellular/WIFI
3	Communication between Mobile Device and the BLEM	RF via BLE
4	Communication between Vehicle SDN and TCU	FTCP via Cellular
5	Communication between CVPODS and Vehicle SDN	HTTP(S)
6	Communication between CVPODS and Common SDN	HTTP(S)
7	Communication between CVFMA and Vehicle SDN	HTTP(S)
8	Communication between CVFMA and SSP	HTTP(S)
9	Communication between CVFMA and CVPODS	HTTP(S)
10	Communication between IVSS Cloud and CVPODS	HTTP(S
11	Communication between IVSS Cloud and IVSS Core	HTTP(S
12	Communication between IVSS Core and GiVIS	HTTP(S)
13	Communication between IVSS Core and GVMS	HTTP(S)
14	Communication between GiVIS and GVMS	HTTP(S)
15	Communication between CRC and CVPODS	HTTP(S)
16	Communication between BLEM and ECG	Multiplex packet exchange via CAN (FD2_CAN)
17	Communication between CVFMA and CVBOP	HTTP(S)
18	Communication between CVFMA and Vehicle Profile	HTTP(S)
19	Communication between Vehicle Profile and xAPI	HTTP(S)
20	Communication between ECG and RGTM	Multiplex packet exchange via CAN (MS2_CAN)
24	Communication between BCM and ECG	Multiplex packet exchange via CAN (FD1_CAN)
25	Communication between SYNC (Phoenix) and ECG	Multiplex packet exchange via CAN (HS3_CAN)
26	Communication between TCU and ECG	Multiplex packet exchange via CAN (FD2_CAN)
27	Communication between Cluster (SYNC Phoenix) and ECG	Multiplex packet exchange via CAN (HS3_CAN)
21	Communication between CVFMA and GVMS	HTTP(S)

22	Communication between eCats/Dealer and GiVIS	FTP/HTTP(S)
23	Communication between GecHub and GiVIS	FTP/HTTP(S)
27	Communication between V-SDN and GVMS	HTTP(S)

Table 15 PaaK Interfaces Descriptions (FNV3)

8 SEQUENCE DIAGRAMS

8.1 Off Board Diagrams:

8.1.1 PaaK Reset

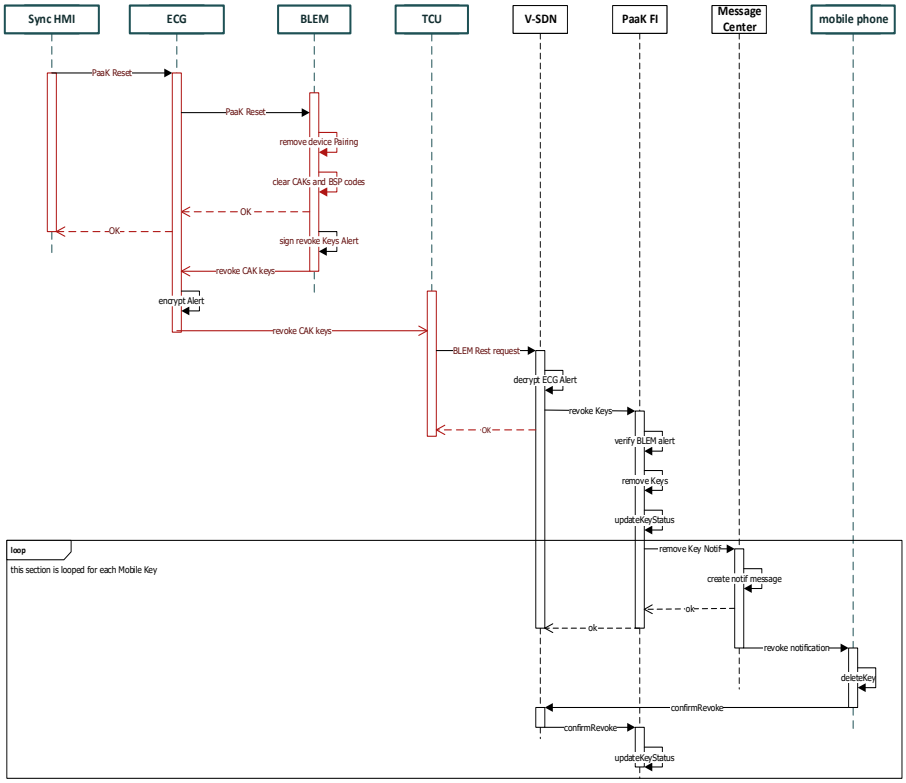


Diagram 3 FNV2 PaaK Reset Sequence Diagram

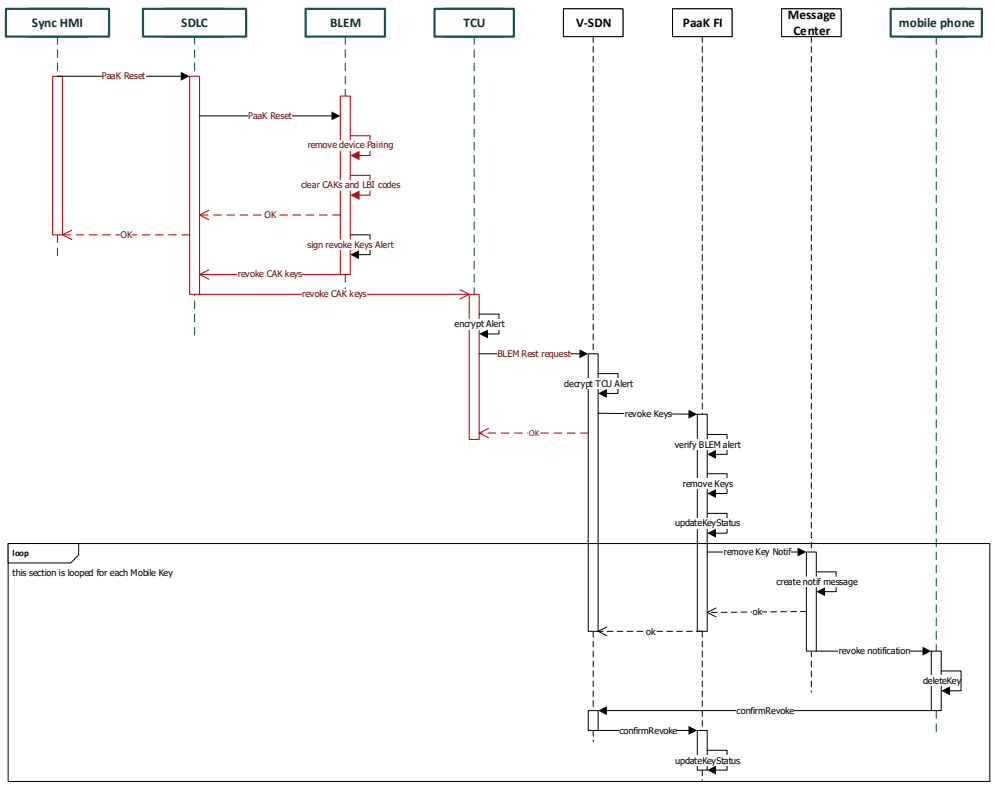


Diagram 4 CGEA PaaK Reset Sequence Diagram

8.1.2 **Master Reset**

Figure 8: FNV2 Master Reset Sequence Diagram

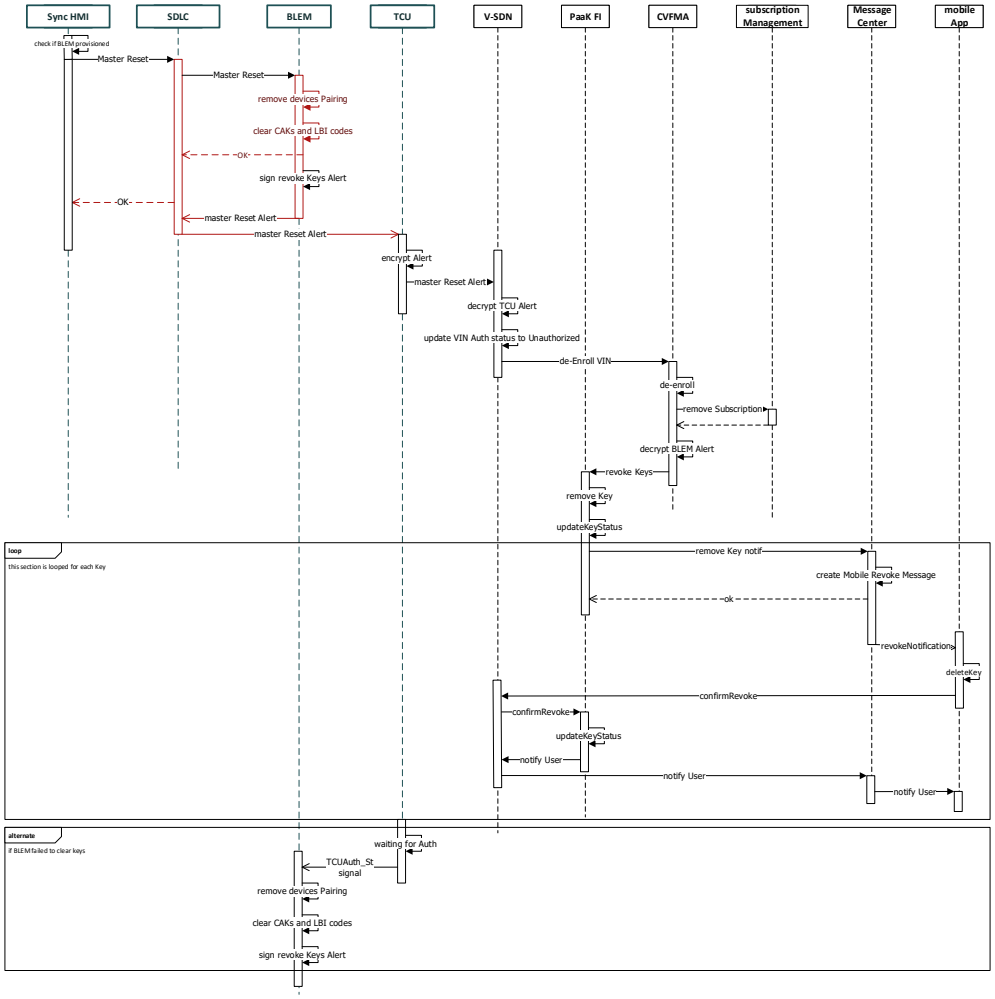


Diagram 5 CGEA Master Reset Sequence Diagram

8.1.3 **Vehicle Removal**

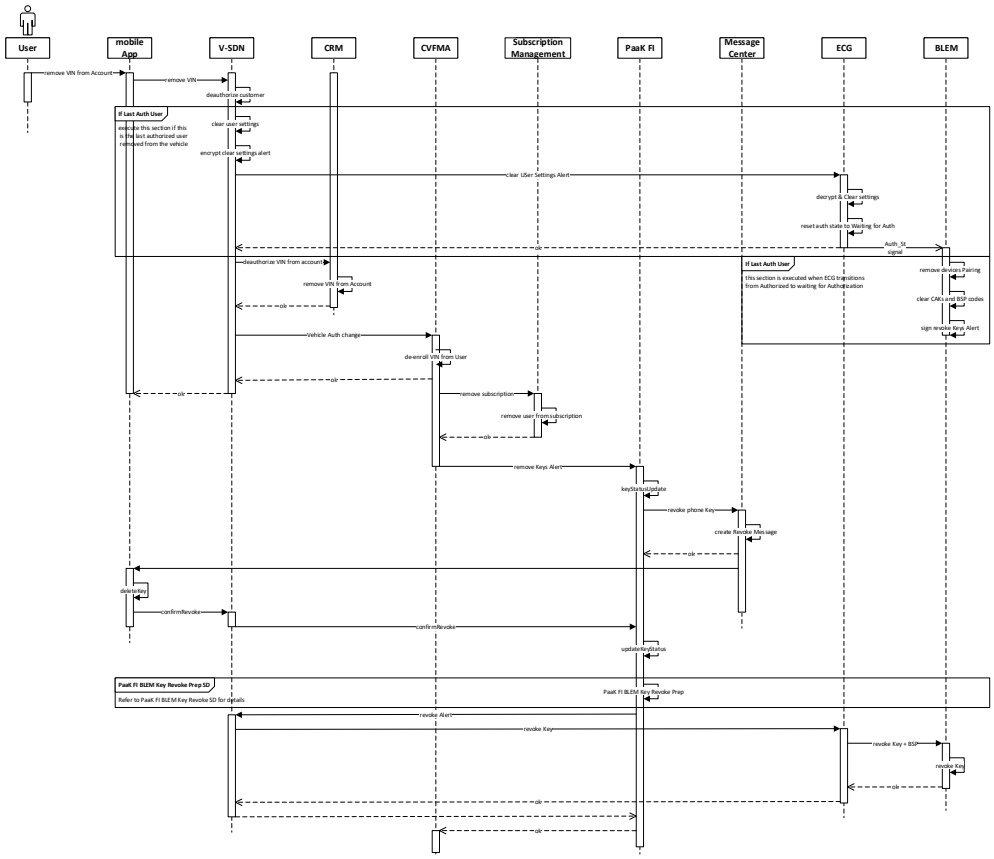


Diagram 6 FNV2 Vehicle Removal Sequence Diagram

Diagram 7 CGEA Vehicle Removal Sequence Diagram

8.1.4 **PaaK FI BLEM Key Revoke Prep**

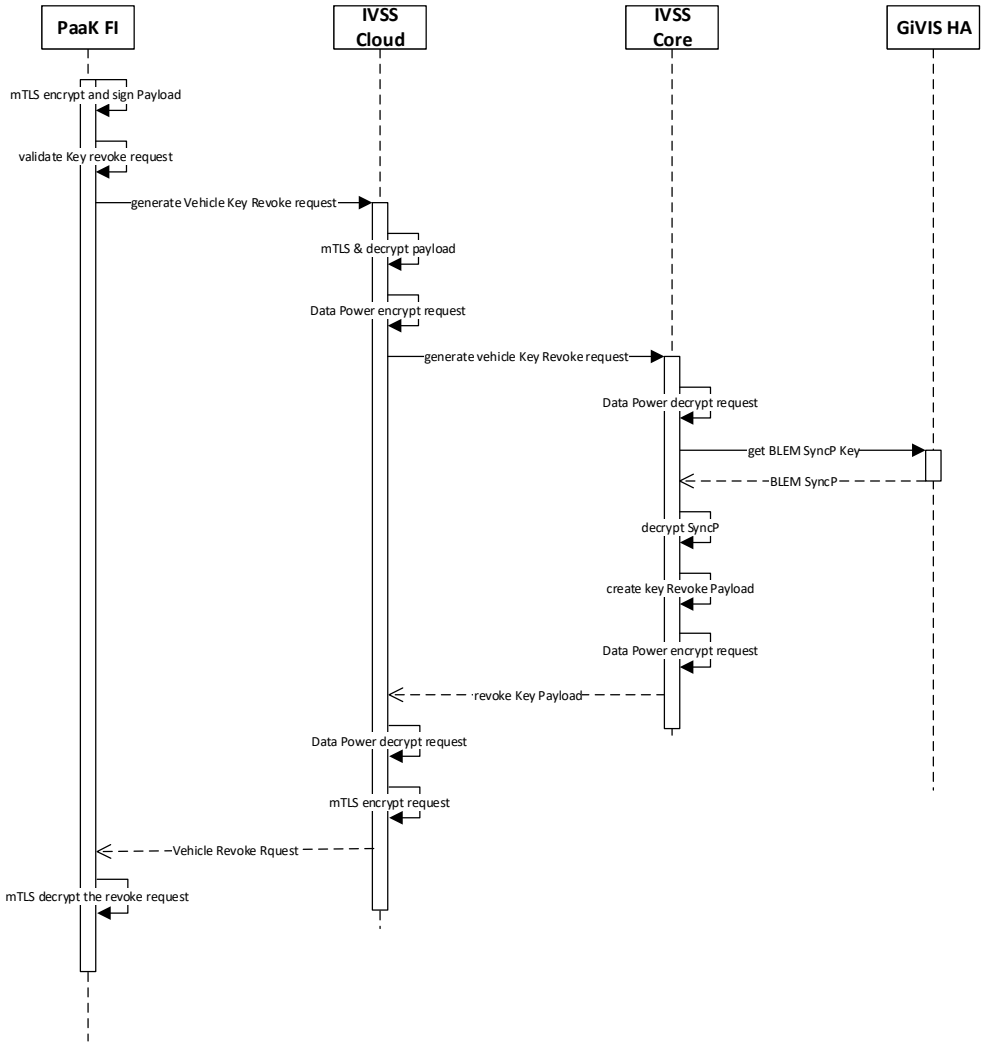


Diagram 8 PaaK FI BLEM Key Revoke Prep Sequence Diagram

8.1.5 **Key Management**

For Key Request, Key Revoke, Key State and Key Generate, refer to the Sequence Diagrams in the Key Management PSD

8.2 On Board Diagrams

Refer to PaaK Sequence Diagrams

8.2.1 Key Delivery and Initial Pairing

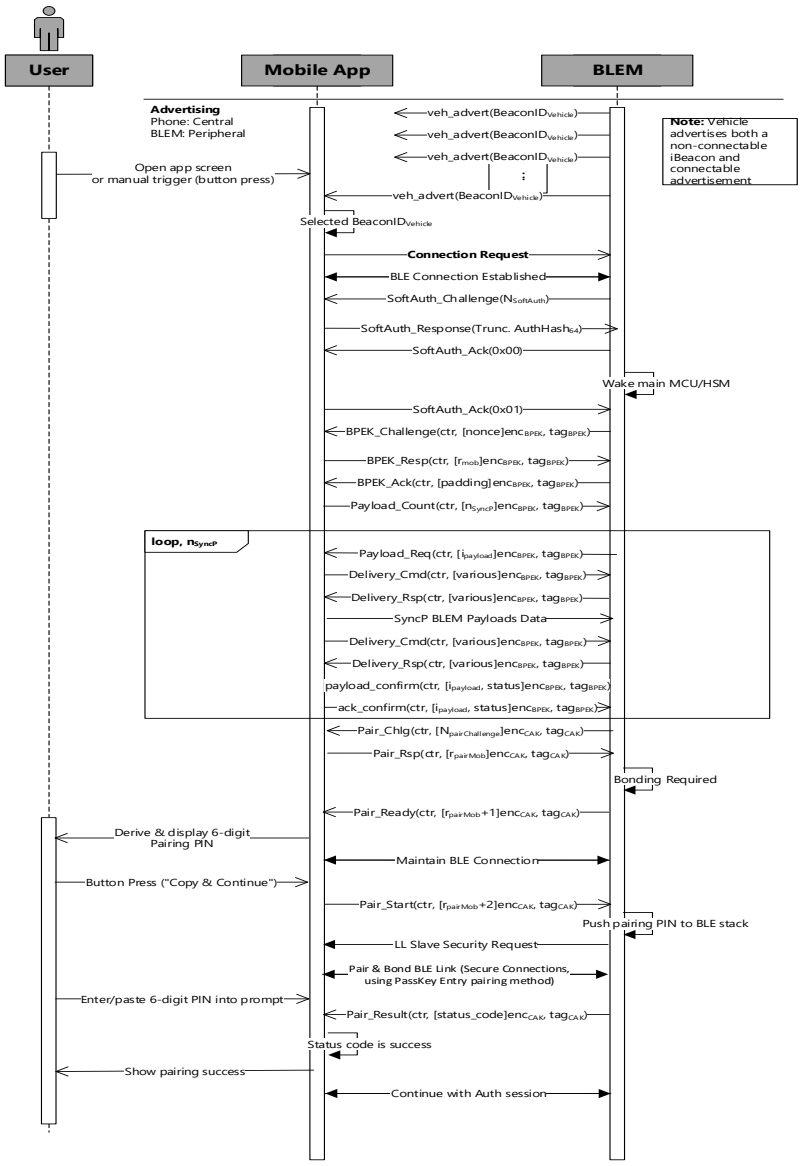


Diagram 9 Key Delivery and Bonding

8.2.2 BLE subsequent connection

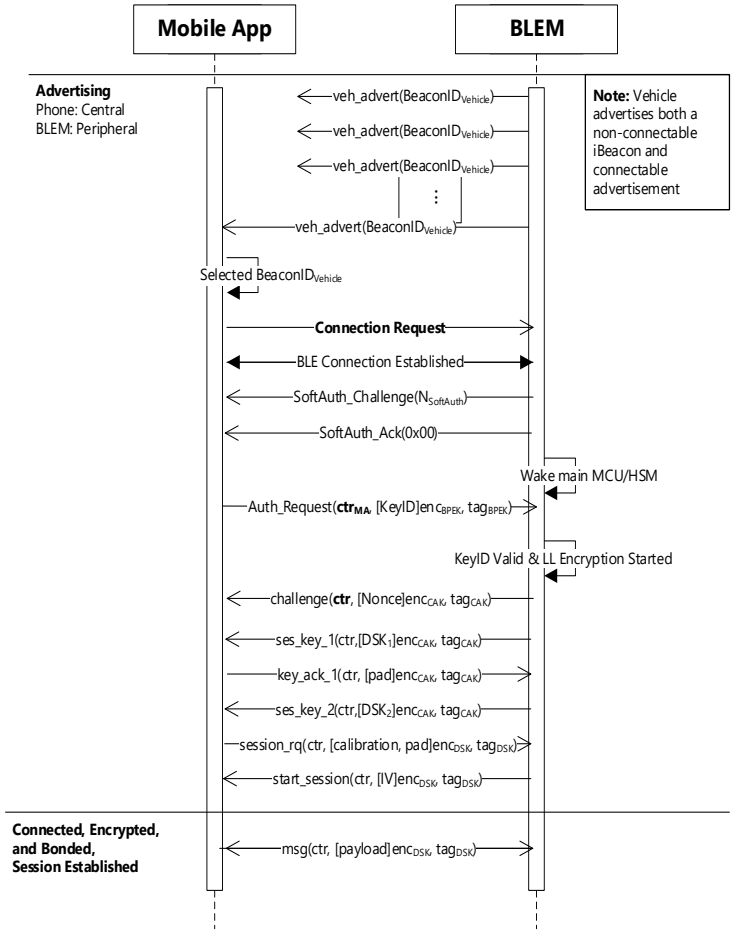


Diagram 10 BLE subsequent connection Sequence Diagram

8.2.3 Active Commands

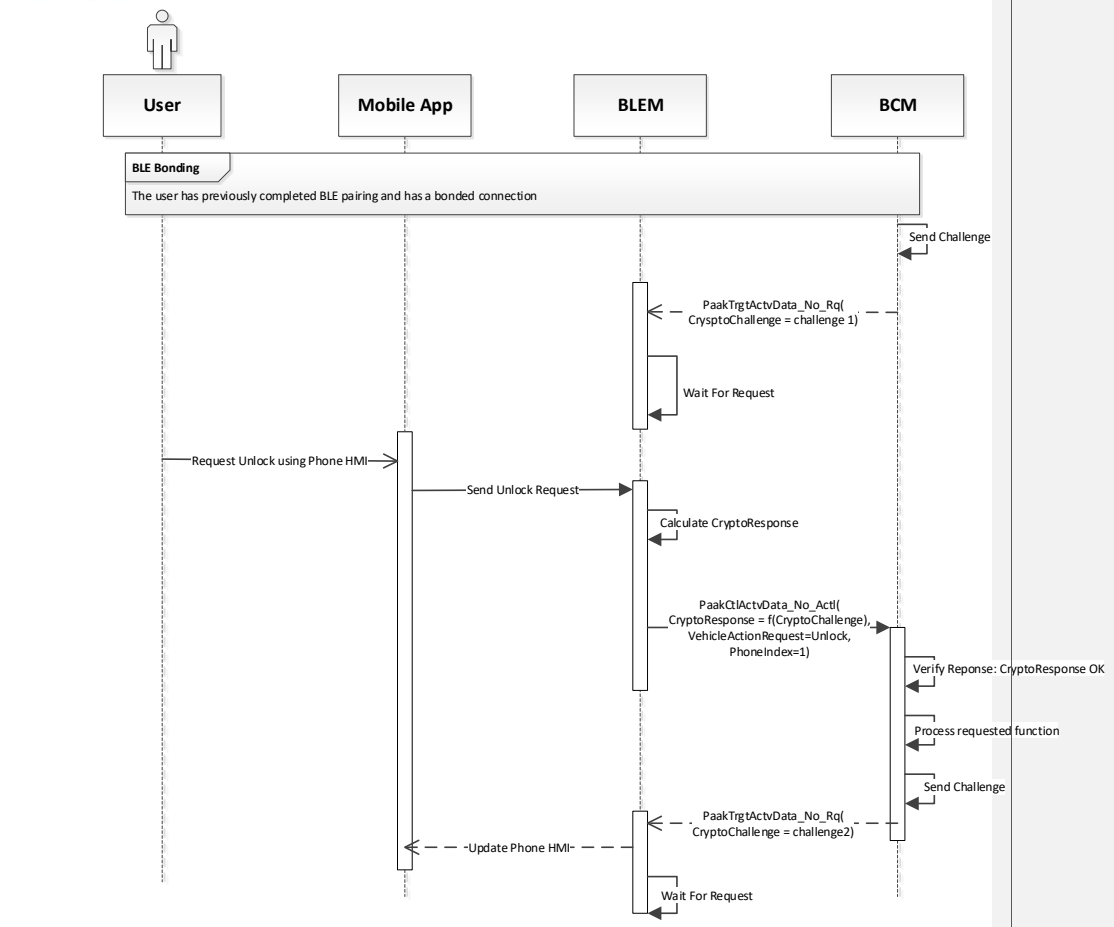
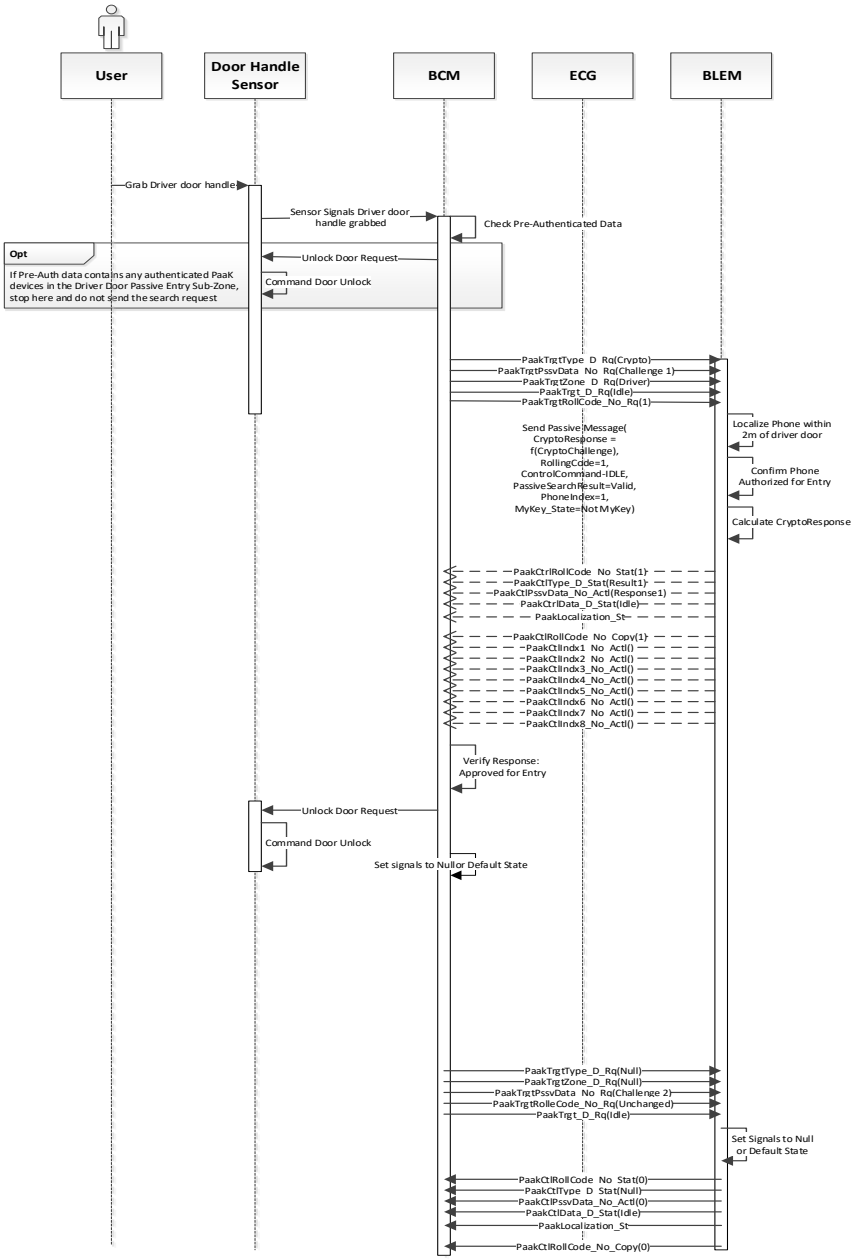


Diagram 11 Active Commands Sequence Diagram

8.2.4 **Passive Commands**

Feature Document

PaaK



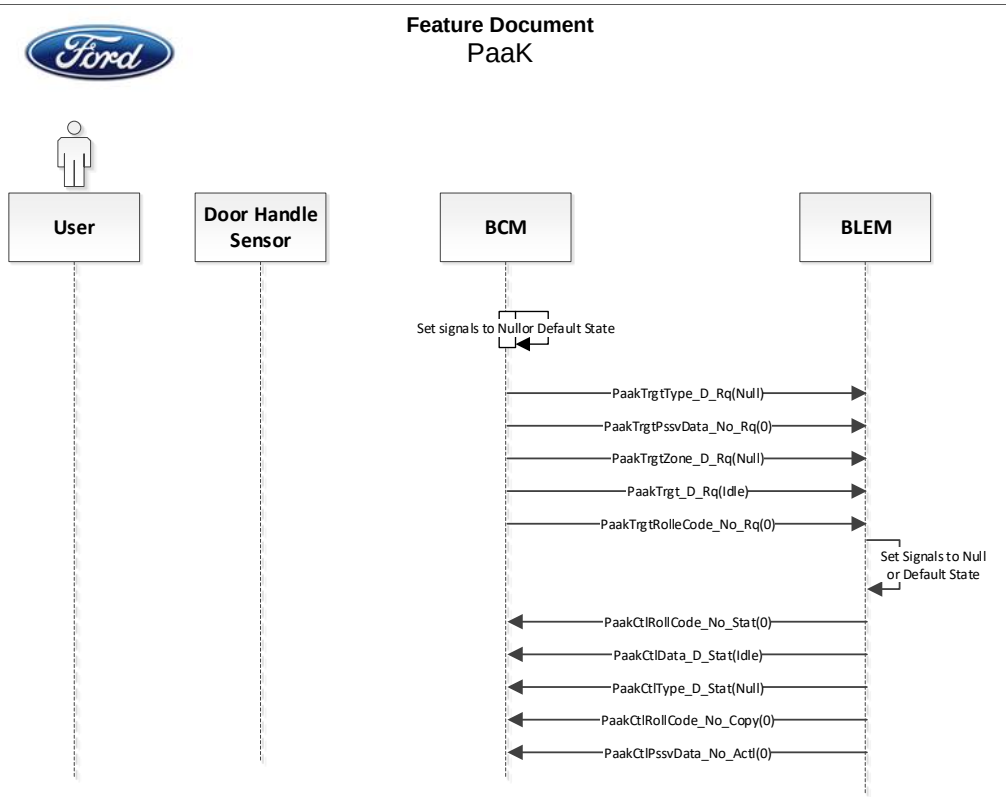
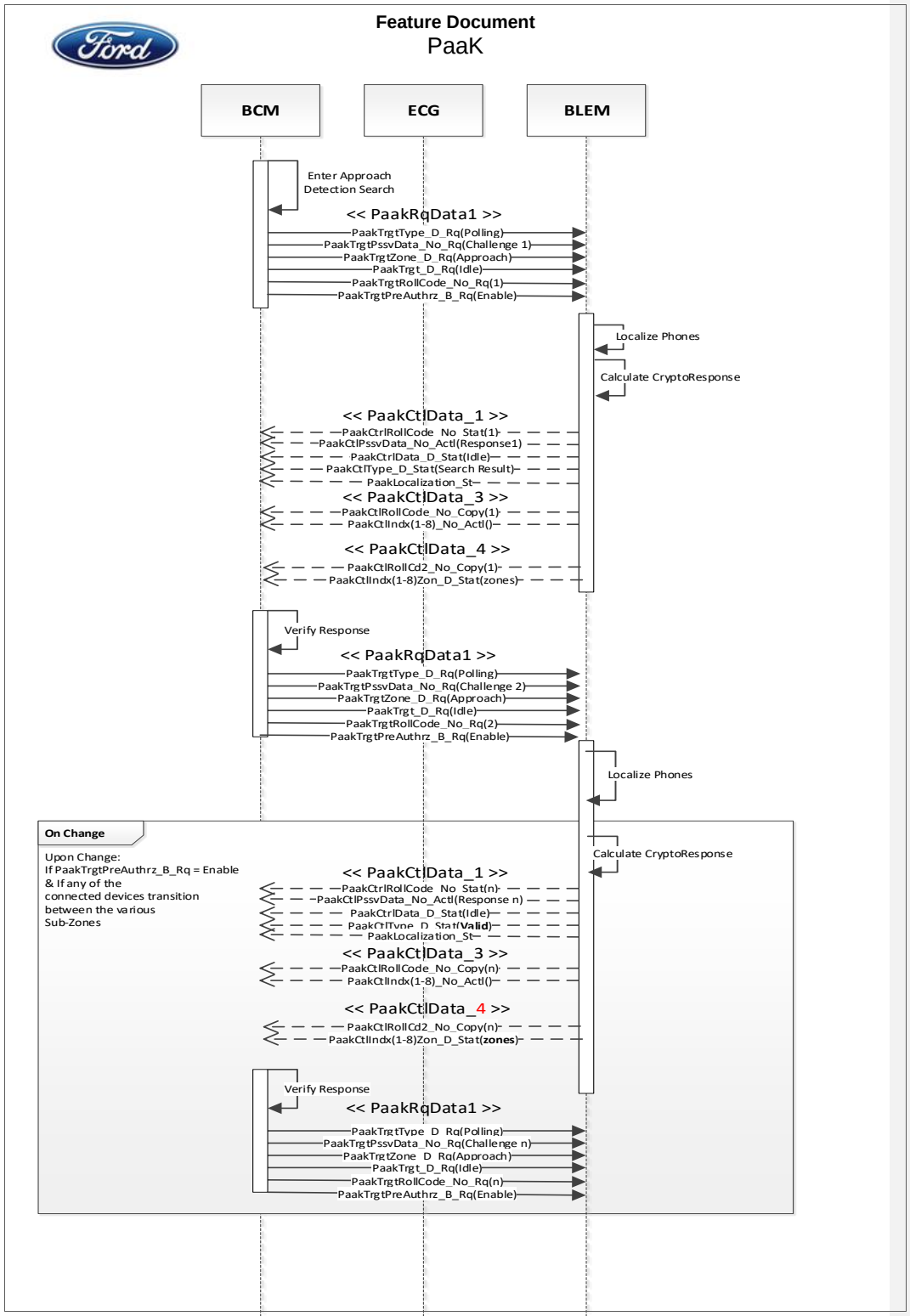


Diagram 12 Passive Commands Sequence Diagram

8.2.5 **Approach Detection**

Feature Document

PaaK



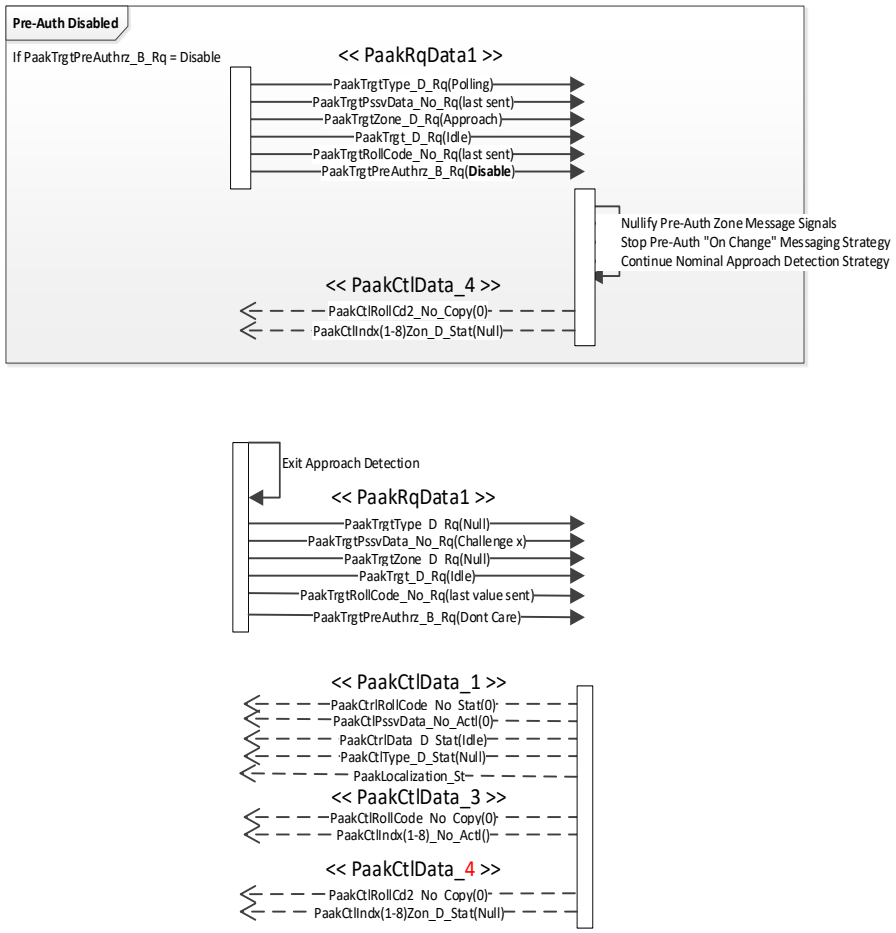


Diagram 13 Approach Detection diagram

8.2.6 **Target ID Transfer**

Feature Document

PaaK

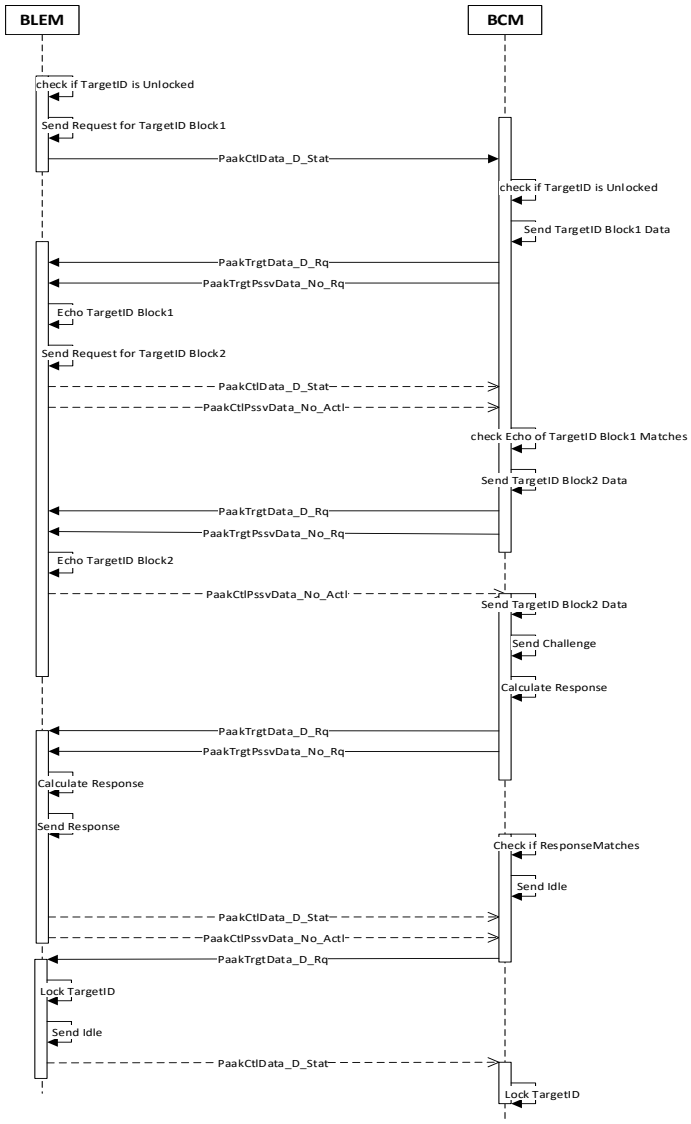


Diagram 14 Target ID Transfer Sequence Diagram

8.2.7 BLEM Provisioning

Feature Document

PaaK

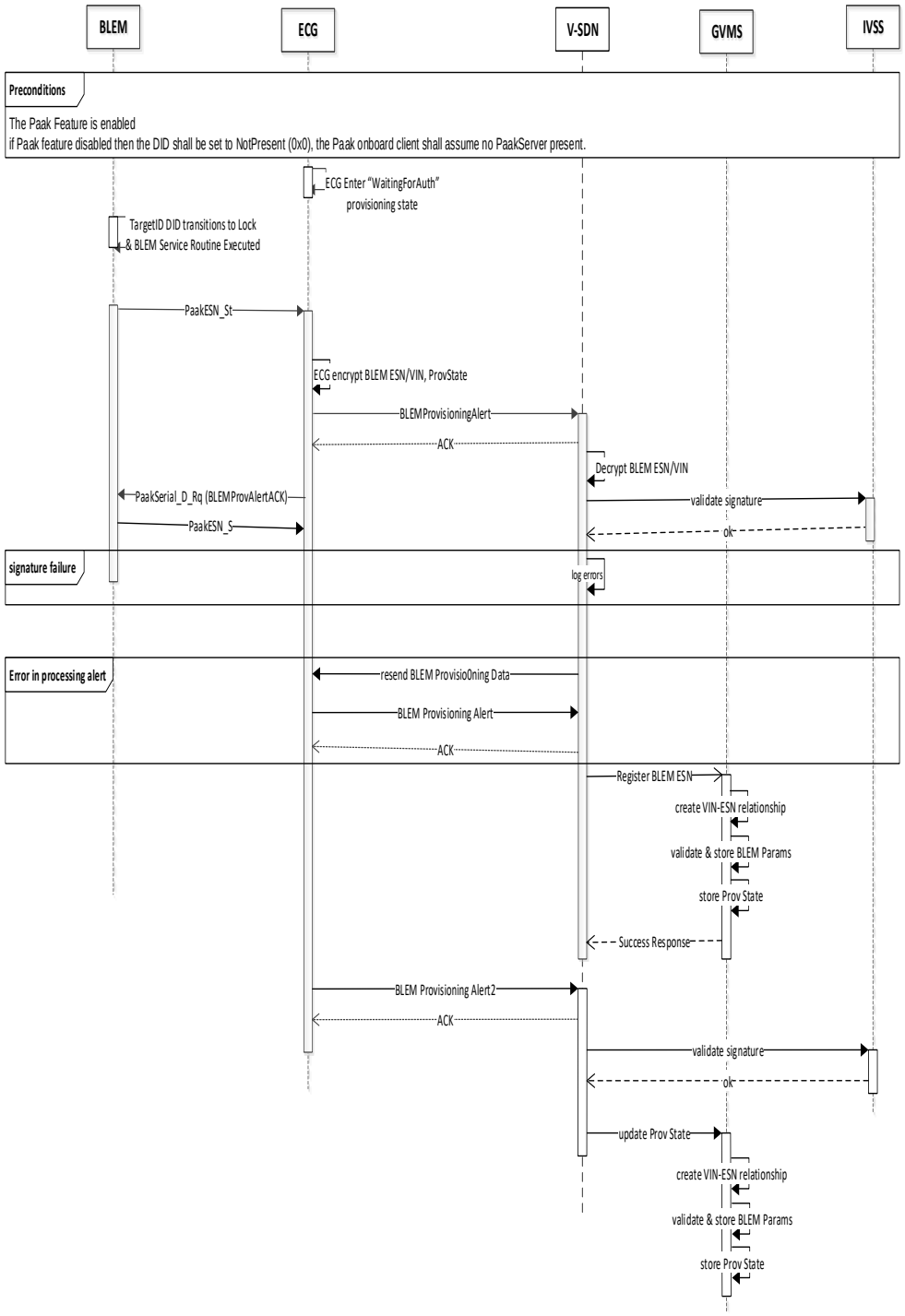


Diagram 15 FNV2 BLEM Provisioning Sequence Diagram

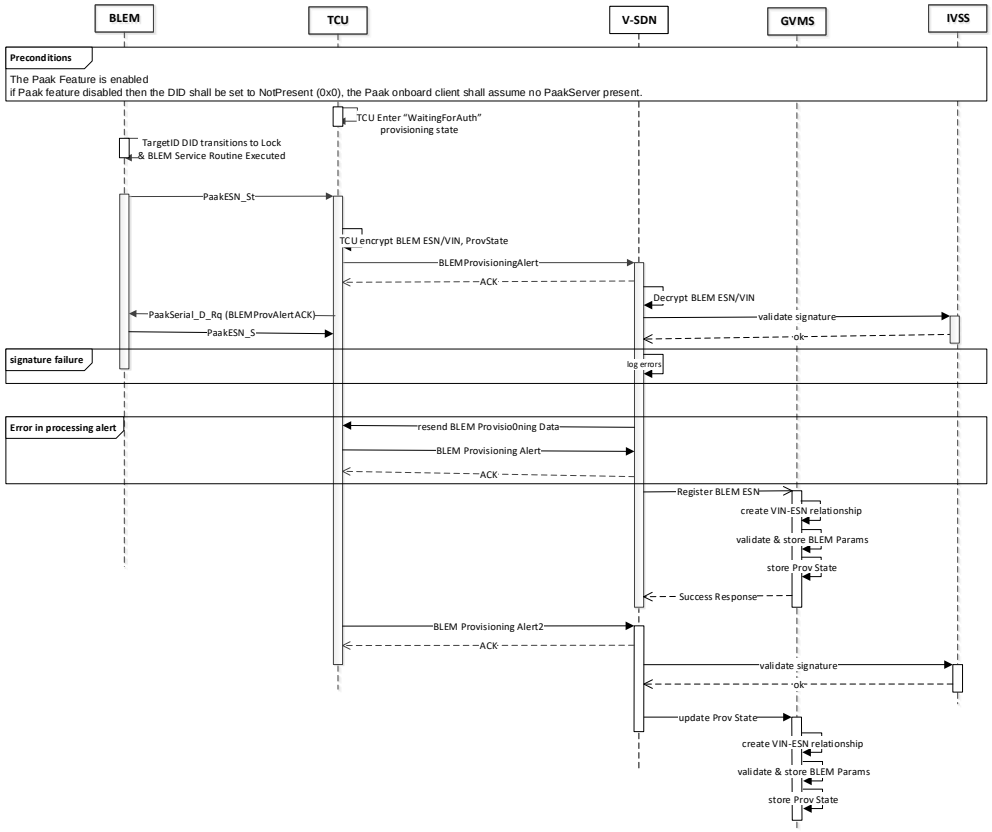


Diagram 16 CGEA BLEM Provisioning Sequence Diagram

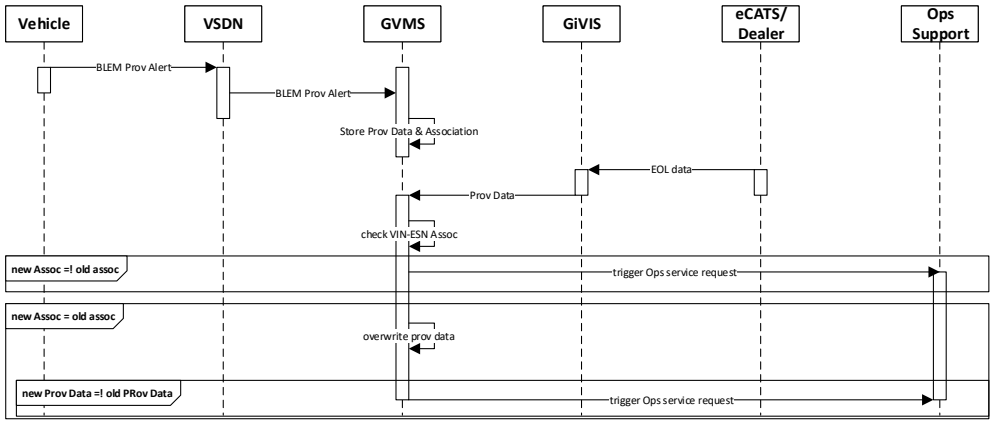


Diagram 17 BLEM OffBoard Data Acquisition and Validation

8.2.8 **Enhanced Memory**

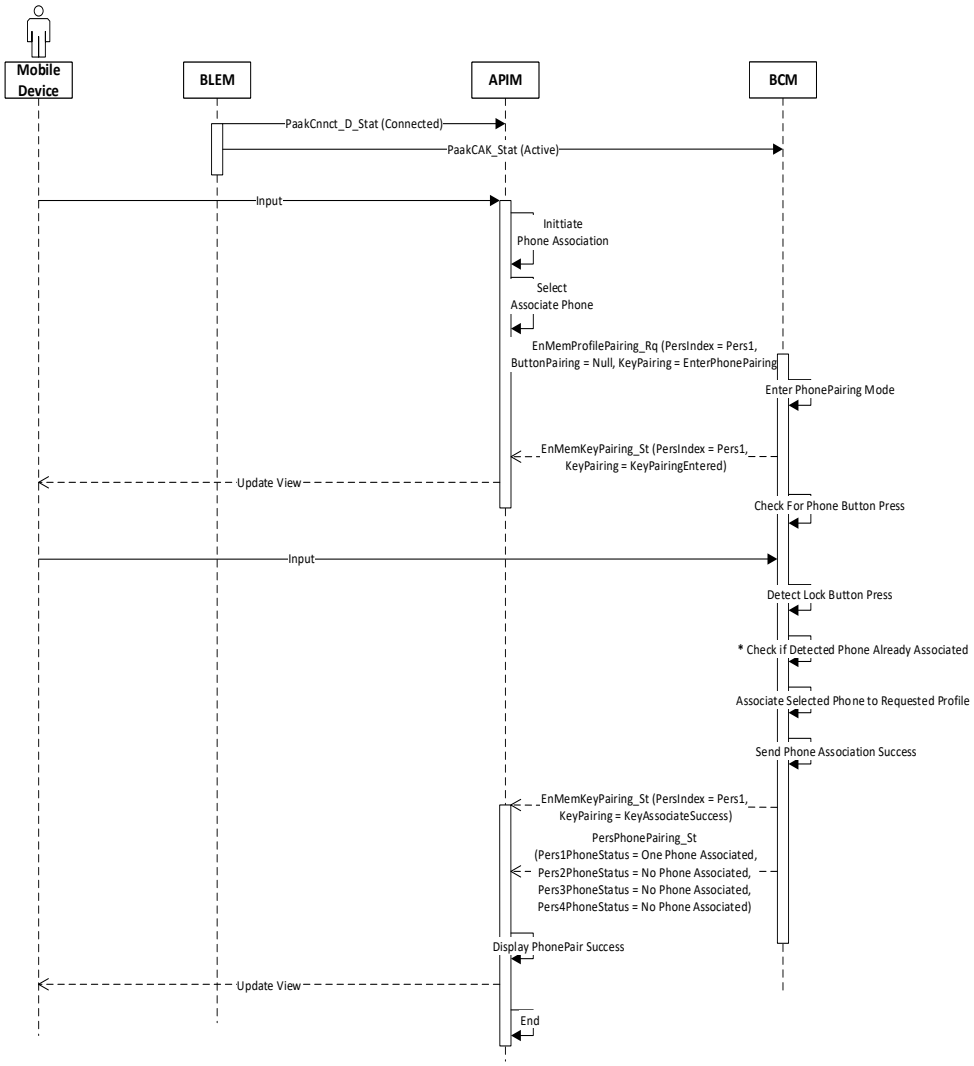


Diagram 18 Enhanced Memory Sequence Diagram

8.2.9 **MyKey**

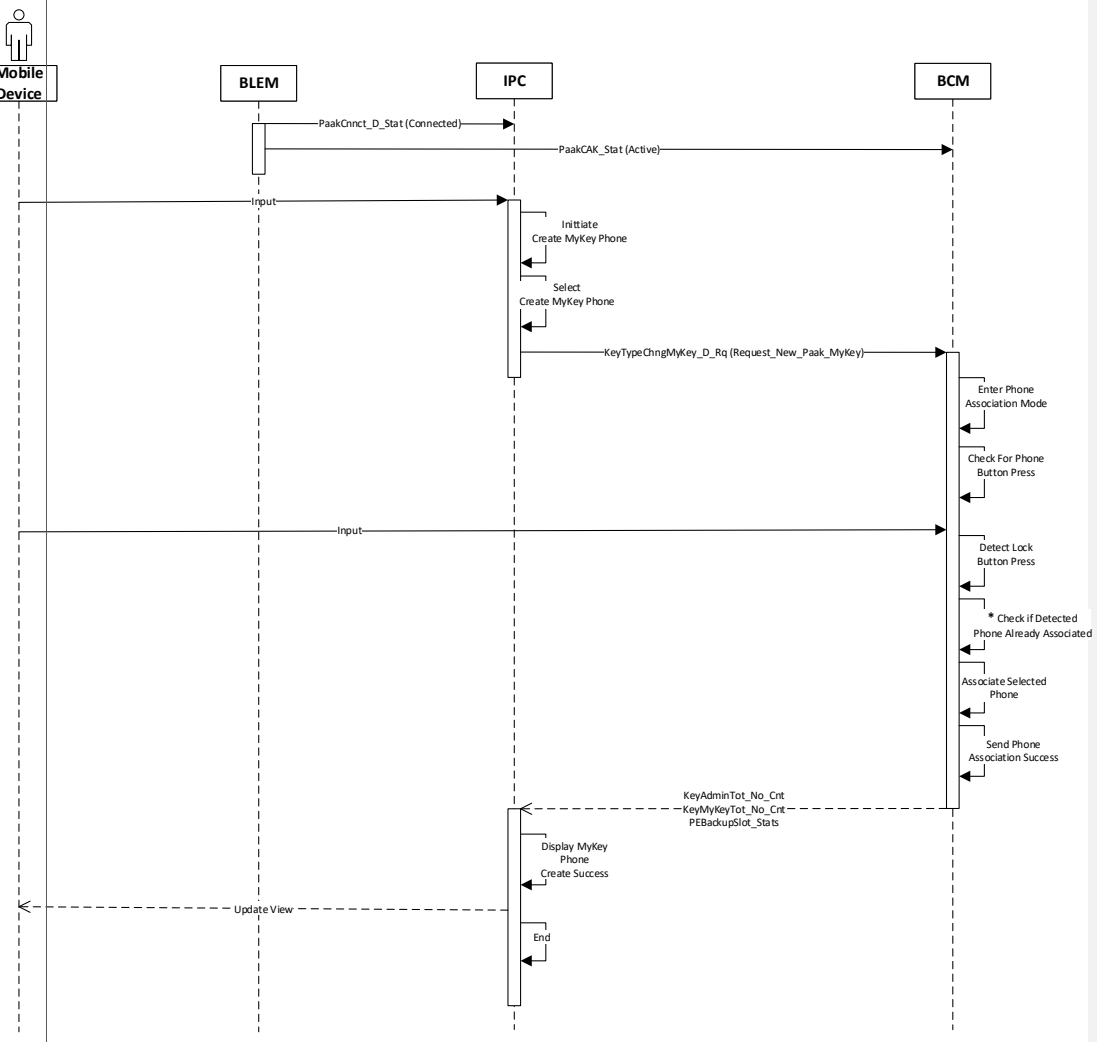


Diagram 19 My Key Sequence Diagram

8.2.10 **BLEM Replacement**

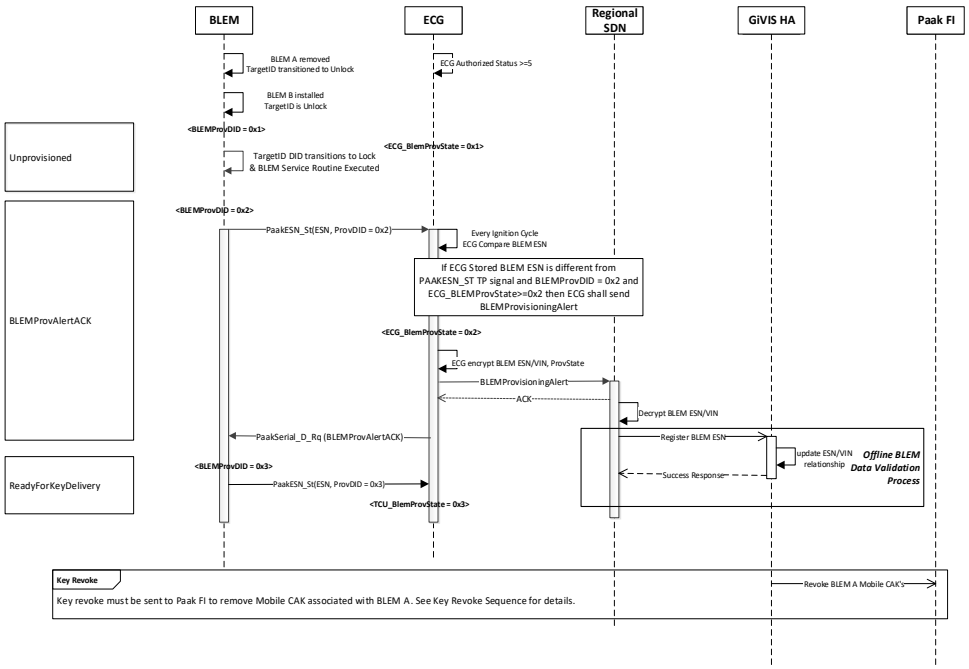


Diagram 20 FNV2 BLEM Replacement Sequence Diagram

Diagram 21 CGEA BLEM Replacement Sequence Diagram

8.2.11 **Initial Pairing**

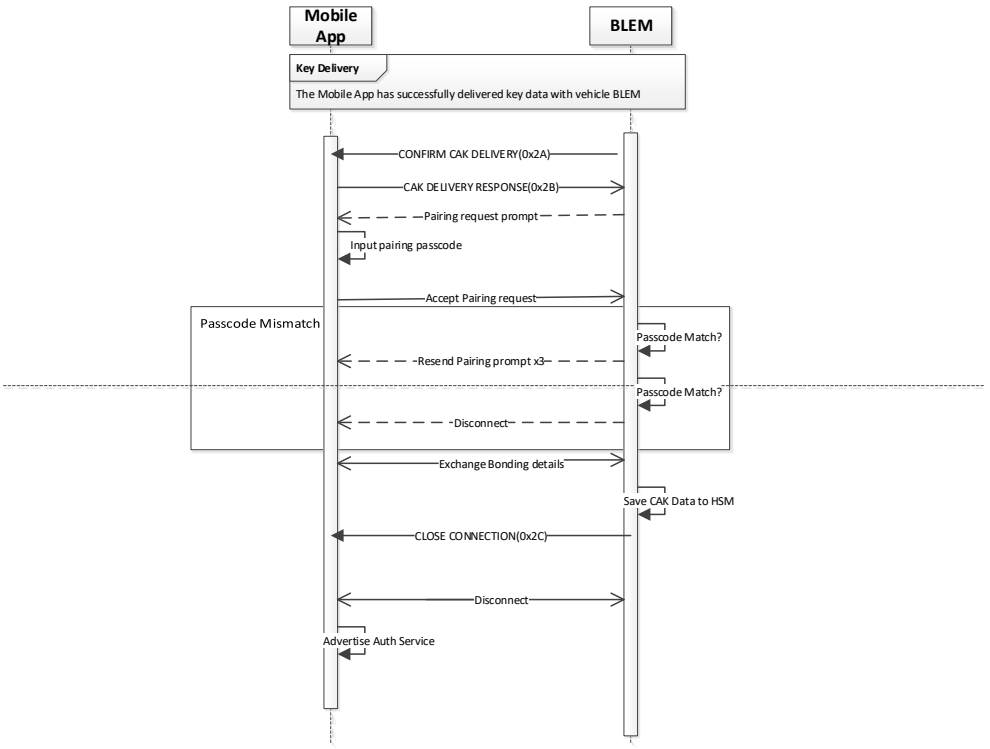


Diagram 22 Initial Pairing Sequence Diagram

9 FUNCTIONAL REQUIREMENTS

9.1 System Setup

###F_PaaK_R_00001### PaaK Initialization

As a prerequisite for the PaaK feature to be commercially available, the following processes shall be completed in the final assembly process:

- Supplier has successfully sent and Ford IT has processed metadata for the BLEM.
- Target ID process on BLEM and BCM
- BLEM/BLEAM self-test.
- PaaK Feature is enabled such as BCM, BLEM, Sync, TCU and ECG (FNV2, 3)

###F_PaaK_R_00002### Target ID Transfer

A Target ID Transfer process shall be initiated for the BLEM in order to transfer secure data & authenticate communications between the BCM & BLEM.

Preconditions:

- BLEM and BCM installed in the vehicle.
- Both BLEM and BCM shall be in an unlocked state

All BLEM modules provided by the supplier to Ford Assembly plants shall be in an unlocked state. Once the BLEM is installed into the vehicle, it shall utilize the Target ID Transfer routine/process and "marry" itself to BCM module.

The Target ID Transfer process works as follows:

- The BLEM starts by requesting the first half of TargetID from BCM
- BCM responds back with the first half of the TargetID,
- BLEM echoes the first half of the Target ID and sends a request for the second half of the Target ID to BCM,
- BCM check the echo of the first half of the TargetID and delivers to the BLEM the second half of the TargetID through the same process as for the first half,
- the BLEM receives the challenge, calculates the response and sends back results to BCM,
- the BCM checks the challenge response and confirms back to BLEM,
- both BCM and BLEM store the TargetID and transition their states to locked.

###F_PaaK_R_00003### ECU Configurable Parameters for PaaK

PaaK shall support ECUs configurations that shall be set in the manufacturing process. ECU's that will support configurations for PaaK are:

1. BCM Configuration

   The BCM shall have a configuration Parameter to enable/disable PaaK. Refer to BCM Part2 specs for details

2. BLEM Configuration

The BLEM shall have a configuration Parameter to enable/disable PaaK. Refer to BLEM Part2 specs for details

3. TCU Configuration (CGEA)
   The TCU shall have a configuration Parameter to enable/disable PaaK. Refer to TCU Part2 specs for details.

4. ECG Configuration (FNV2, 3)
   The ECG shall have a configuration Parameter to enable/disable PaaK. Refer to ECG Part2 specs for details

5. Sync
   Sync shall have a configuration Parameter to enable/disable PaaK. Refer to SYNC Part2 specs for details

9.1.1 Supplier Feed

###F_PaaK_R_00004### BLEM Supplier Feed for PaaK

The BLEM Supplier shall generate its own security certificates and keys (SynckP key and BPEK key)

The BLEM supplier shall create and provide BLEM metadata to Ford which will feed downstream applications: The supplier shall generate the following module-specific data as part of the production process, but not limited to: ESN number, BUUID, iBeacon UUID, BT MAC Address, Resend Flag, assembly part number, core assembly part number, strategy part number, calibration part number, signal configuration part number, plant ship, date, destination region code, manufacturing facility code, BLEM Pre-Shared Secret Keys (SYNCP Key, BPEK key), etc.

The following systems are involved in the supplier feed process:
1. BLEM Supplier.
2. FORD-GEC Hub: GEC Hub is the Global Electronic Commerce Hub used by both BLEM Supplier and Ford Systems to exchange the Supplier Feed and Response files.
3. GVMS supplier feed scheduler service will periodically process the GEC Hub Mailbox and send the information to IVSS if it finds a new supplier feed file.

Refer to the Supplier Feed Spec for more details.

###F_PaaK_R_00005### BLEM symmetric key

The Supplier shall use a FIPS 140-2 compliant HSM to generate the symmetric keys.

###F_PaaK_R_00006### BLEM Supplier Feed File preparation

The data shall be extracted from the database, encoded in the XML format by complying with XML Schema definition. The supplier feed file shall be validated to comply with XML schema definitions prior sending to Ford.

The XML payload shall be signed by the supplier using a private certificate generated and managed by the supplier. The XML payload shall then be encrypted using the public certificate provided by Ford
The Supplier shall drop the signed and encrypted file at GEC Hub Inbox

###F_PaaK_R_00007### BLEM Supplier Feed File handling

The Supplier shall read the response XML from GEC Hub Outbox and process every module's response data. The response data shall be stored at supplier's Manufacturing plant database. In case of supplier feed process fails there shall be a retry mechanism to reprocess the feed.

For more details, refer to the Supplier Feed Spec.

9.1.2 Provisioning

###F_PaaK_R_00008### BLEM Provisioning

Once a BLEM is installed in the vehicle and power is detected by the BLEM, the BLEM shall start the provisioning process with onboard modules such as BCM, and TCU (CGEA) or ECG (FNV2, 3)), and off-board systems. The provisioning process shall be successfully completed before a user can request a CAK.

Pre-conditions:

- ECG and/or TCU provisioning completed,
- Target ID Transfer process between BLEM and BCM completed,
- BLEM Supplier feed already ingested in GVMS,
- The BLEM DID status checked in manufacturing plant to ensure it is in un-provisioned state.

###F_PaaK_R_00009### BLEM Provisioning process

The BLEM provisioning process is as follows:

- The BLEM shall begin to send the ESN TP message after a service routine is performed causing the BLEM to transition the TargetID DID from unlocked to locked. This message must include the BLEM ESN, the BLEM ProvDID, and configuration parameters (see BLEM SPSS for list of parameters).
- TCU (CGEA) or ECG (FNV2, 3) then sends the BLEM ESN, the BLEMProvState param and the configuration parameters to the cloud in a provisioning alert.
- If error conditions (Data lost, data corrupted, Invalid signature, etc.) happen, the cloud shall send a BLEM Provisioning Request Command to the TCU (CGEA) / ECG (FNV2, 3) to get the provisioning data again. TCU / ECG shall resend the data without requesting additional data from the BLEM.
- BLEM receives a "BLEM provision alert Acknowledgement" from the cloud and transitions its status to "BLEMWaitForKeyAlert", and send a message to TCU / ECG to update its status to ready for key delivery
- Provisioning from the Vehicle is then routed by V-SDN first to IVSS for BLEM SyncP signature validation, then to GVMS so that VIN to BLEM ESN mapping can be established/maintained and BPEK hash verified against the stored value. GVMS also stores the received configuration data.
- GiVIS Core will re-affirm the VIN to BLEM ESN Mapping with GVMS once EOL processing is completed for the assembly plant. If a mismatch is found GVMS shall keep its VIN-ESN mapping and trigger a service request.
- The plant shall check for the BLEM "BLEMWaitForKeyAlert" state.
- If the BLEM receives an error message back from the TCU / ECG it resets its provisioning DID to "un-provisioned" and restarts the process over again.

See BLEM Provisioning SPSS, TCU SPSS and ECG SPSS documents for detailed information.

9.1.3 PaaK Auto Subscribe

###F_PaaK_R_00010### PaaK Auto Subscribe

Auto subscribe is the process where upon TCU (CGEA) or ECG (FNV2, 3) authorization being completed the IT backend triggers the PaaK subscription to be created in SuMo for the customer and enrollment in PaaK in CVFMA.
This is done without any customer interaction besides completing the TCU (CGEA) or ECG (FNV2, 3) authorization process which includes the acceptance of the terms and conditions upon the mobile app download.

Pre-Conditions to PaaK Auto Subscribe:

- Mobile App shall be installed and the customer created a user account
- VIN is authorized against the TCU (CGEA) or ECG (FNV2, 3)
- User has a VIN that is PaaK capable added to his account

ECG / TCU / BCM / BLEM need to be properly installed and provisioned
The PaaK terms and conditions shall be contained within the mobile app terms and conditions.

PaaK FI shall store authorized VIN along with associated mobile App ID.

A single subscription shall be created for a VIN, the name on the subscription is the first user to claim it.

All authorized users that enroll in PaaK shall have their name associated to the single subscription
The user shall be able to add multiple vehicles with PaaK capability to the same user account. There is not a limit to the number of vehicles a customer can have in his account.

When new owner authorizes the TCU (CGEA) or ECG (FNV2, 3) this shall trigger the auto subscribe process for PaaK.
The first user shall complete the authorization process by accepting the T&C on SYNC display inside the vehicle

This authorization shall trigger the app to send the Mobile Public Key to PaaK FI. This shall occur when first VIN is authorized..

Subscription shall be cancelled upon Master Reset, or Brand Reset.
Subscription shall not be cancelled upon a PaaK Reset or upon CAK Revoke.

Subscription shall be cancelled when last authorized user removes his VIN from account.

If first user either removes the VIN from his account or de-authorizes the TCU (CGEA) or ECG (FNV2, 3) the subscription shall be updated to be in the name of the next authorized user on the list.

Once the above auto subscribe process is completed the customer shall be able to initiate a CAK request.

###F_PaaK_R_00011### PaaK Auto Subscribe Process

The following steps explain the Auto subscribe process:

1. CVFMA sends SuMo authorization events.
2. SuMo calls CVFMA to perform a Vehicle Capability check.
3. CVFMA calls GVMS to fetch BLEM Data for Vehicle Capability check.
4. SuMo determines if the VIN should be subscribed to PaaK based on the Vehicle Capability response from CVFMA.
5. SuMo calls CVFMA to create an enrollment record in PaaK Feature Package with a list of authorized users.
6. CVFMA creates enrollment record and notifies targets (PaaK application would be a target). The notification will include all users that are authorized to the vehicle.

9.1.4 Device Capability check

###F_PaaK_R_00012### Device Capabilities Check

PaaK feature shall be allowed only on mobile devices that meet the following conditions:

- The device type and OS (iOS and Android) versions shall be in the approved list as specified in sections 9.1.9 and 9.1.10
- The Bluetooth version shall meet the specifications in section 9.1.9 an 9.1.10
- During Add Vehicle step and CAK request process, the mobile shall check the above capabilities and report an error message if the conditions are not met, notifying the customer that his phone is not supported.
- The customer shall not be allowed to request CAK if his device is not supported. However he shall be able to get key status and revoke his keys, as per key revoke specifications.

In addition to the above, Jailbroken/rooted device shall be detected whenever possible by the mobile app and customer shall be notified about potential risk of using a jailbroken/rooted device.

- The customer shall be requested to acknowledge Risk acceptance in T&C during mobile app installation
- The phone state (jailbroken or rooted) shall be logged by the app in backend IT systems.
- Ford shall actively monitor threat intelligence, app stores, code repositories, and dark web in order to respond adequately to any potential risks around jailbroken and rooted devices
- The mobile app shall implement additional whitebox encryption for data within the sandbox.
- The mobile app shall implement more frequent whitebox key rotations

IOT (Inter-Operability) Testing is required for all approved smartphones. This testing is to check the compatibility between BLEM and the smart phones. PaaK supported devices will be updated periodically and will be formally approved by Ford. Refer to “PaaK Phone List” specified in section 9.1.7 abd 9.1.8 for list of approved mobile devices for NA, Mexico, Europe and China.
A list of compatible devices shall be made available online to consumers. The list shall be updated quarterly

9.1.5 Testing Support

###F_PaaK_R_00013### PaaK Testing Support

The BLEM shall be able to provide the log of actions performed through Bluetooth communication, such as received RKE commands and sent acknowledgements, localization data, etc.

9.1.6 Number of Devices Supported

###F_PaaK_R_00014### BLEM CAK Upper Limit

BLEM secure storage shall have memory capacity to support no less than **62** slots (CAK keys and BSP passcodes).

###F_PaaK_R_00015### Concurrent Mobile Device Connections

The BLEM shall be capable of accepting connections from all authorized devices and tracking the locations of all authorized Mobile devices concurrently.

###F_PaaK_R_00016### Maximum Active CAK Supported

PaaK feature will support up to **4** keys that are configurable in PaaK FI per vehicle in phase 1.

When configured for 4 keys, if the user tries to request a **5th** key, his request shall be rejected and notified that the maximum number of keys is in use for that vehicle. The customer will be able to request a key after one of the 4 keys already allocated gets revoked.

Refer to Key revoke section for more details on how to revoke an existing key.

9.1.7 Mobile Devices Support

###F_PaaK_R_00017### iPhone Support

The PaaK feature shall work on the iPhone models, which support Bluetooth 4.2 or later and running iOS 8.x or later. For list of approved mobile devices for NA, Mexico, Europe and China, refer to document located in: https://pd1.extspt.ford.com/sites/FordConnectedServices/tcu/Features/Forms/SP10SP16CheckIn.aspx?RootFolder=%2Fsites%2FFordConnectedServices%2Ftcu%2FFeatures%2FPaaK%2F12%20System%20Testing%20and%20Verification%2FPAAK%20Phones%20List&FolderCTID=0x0120000D7201D95D41F749831214F9B8078A19&View=%7BE9EF123C-3FA5-4AC4-B668-946020816375%7D

9.1.8 Android Support

###F_PaaK_R_00018### Android Support

The feature shall work on Android models that support Bluetooth 4.2 or later and running Android OS 8.0 or later. For list of approved mobile devices for NA, Mexico, Europe and China, refer to document located in: https://pd1.extspt.ford.com/sites/FordConnectedServices/tcu/Features/Forms/SP10SP16CheckIn.aspx?RootFolder=%2Fsites%2FFordConnectedServices%2Ftcu%2FFeatures%2FPaaK%2F12%20System%20Testing%20and%20Verification%2FPAAK%20Phones%20List&FolderCTID=0x0120000D7201D95D41F749831214F9B8078A19&View=%7BE9EF123C-3FA5-4AC4-B668-946020816375%7D

9.1.9 Bluetooth Protocol Support

###F_PaaK_R_00019### Bluetooth Protocol Support

The Mobile device shall communicate with the vehicle wirelessly using the Bluetooth Low Energy (BLE) standard as defined in the Bluetooth Core Specification version 4.2 or later. Bluetooth versions anterior to 4.2 shall not be supported due to lack of security requirements.

In the case that a Bluetooth version is higher than 4.2 exist, the BLEM & Mobile device shall be backward compatible with each other.

9.1.10 PaaK Consumer Access Key name

###F_PaaK_R_00020### PaaK Consumer Access Key Name

If a user shall request a CAK, the key shall be given a readable name.

- The name shall be automatically assigned to uniquely identify the user's key for that vehicle.
- The user shall be able to rename the key before sending the key request
- Key name shall be stored and validated in PaaK FI.
- PaaK FI shall enforce uniqueness of the Key name per vehicle.
- Length shall be compatible with SYNC HMI, BLEM storage, and CAN bus limits.
- Key name shall be delivered in the BLEM key payload.

- Key shall not be renamed after it is created.
- The key name shall be used as the device identity in SYNC such as BSP and Enhanced Memory.
- The key names associated to the vehicle shall be displayed in the mobile app regardless of who is the owner of the key

9.1.11 PaaK Consumer Access Key Request

###F_PaaK_R_00021### PaaK Consumer Access Key Request

Pre-Conditions to PaaK key request:

- Mobile App shall be installed and the customer created a user account
- The Vehicle has to be authorized by at least one user before a CAK can be requested.
- User has a VIN that is PaaK capable added to their account
- Device capabilities check is performed for PaaK feature compatibility.
- Vehicle has a backup keyless entry system, BSP.
- The mobile device has internet coverage (connectivity to the cloud) to allow a CAK request.

The mobile app shall allow the user the option to request a key provided the Mobile device is supported and meets all necessary requirements as defined in section "device Capabilities", and the mobile app is connected to the Cloud.
If the user's mobile device is not supported the mobile app shall alert the user that his mobile device does not support PaaK feature.
The mobile app shall display the key status of the existing keys to the user before allowing a new key to be request. This will allow the user to be aware of an existing key for the same vehicle and decide to keep it or revoke it.
The mobile app shall not allow a user to request second or more keys for the same vehicle on the same device.
The user shall be required to enter a security object (PIN, passwd, etc.) upon requesting a key.
Consumer Access Key (CAK) request by the user shall initiate the system to create a key pair, with a vehicle component and mobile component.

Refer to *Key Management PSD document* for more details

###F_PaaK_R_00022### PaaK Consumer Access Key delivery to the Phone

Both the mobile device key and the vehicle key shall be delivered to the phone from which the request originated.
A BLEM Payload Exchange (BPEK) shall also be provided by the cloud to the mobile device to be used for authorization process described below.

The mobile device key shall be installed in the mobile device and the vehicle key shall be cached in the mobile device until it gets delivered to the vehicle

###F_PaaK_R_00023### PaaK Consumer Access Key delivery to the Vehicle

The vehicle key shall be delivered to the vehicle by the phone through BLE connection. It is not required to have vehicle TCU connectivity during the key delivery process, as the vehicle key will be delivered through BLE channel.
The Mobile app shall automatically trigger delivery of the Key when it gets within range of the vehicle.

The Mobile device shall be authorized by the BLEM before delivering the CAK to the vehicle. The authorization process shall rely on the BLEM Payload Exchange Key (BPEK), preinstalled in the BLEM by the supplier, and provided to the Mobile device by the cloud.

If the user logs out from the mobile app before delivering the key to the vehicle, the Mobile App shall delete the vehicle CAK SyncP message and its BPEK, delete the Mobile CAK and its corresponding data (Salt, metadata).

The BLEM shall accept a key delivery from a known mobile phone which has previously bonded. If the phone connects to the BLEM and responds to a soft authentication request with a soft Authentication acknewledgement the BLEM shall transition to a Key delivery mode. If the mobile device responds to a soft Authentication request with an session authentication request , the BLEM shall establish a Device Session Key. See Paak BLEM SPSS document for more details on Soft Authentication

###F_PaaK_R_00024### PaaK Consumer Access Key delivery confirmation

The Mobile App shall allow 48 hours for the CAK to be delivered to the vehicle.

At the expiry of the 48 hours, if the mobile app didn't deliver the CAK to the vehicle, the Mobile App shall delete the CAK SyncP message and its BPEK, delete the Mobile CAK and its corresponding data (Salt, metadata) and report a delivery time expiry failure to the cloud. The PaaK FI shall then update the key status accordingly.

If the BLEM reports an error message back to the mobile device, the mobile device shall delete the mobile key and its related data and send back a delivery failure to the cloud.

If PaaK FI does not receive a confirmation back, it shall keep the key status as pending delivery until it receives a confirmation either from the vehicle or the mobile device, or it receives a master or PaaK reset alert from the vehicle or the user removes the VIN.

A delivery confirmation shall be generated from both the mobile device and the vehicle after pairing process is completed. Whichever confirmation comes first to the cloud shall be considered valid and PaaK FI shall update the key state accordingly.

The BLEM shall store the CAK in its HSM system and acknowledge the receipt of the key to the backend system as soon as TCU connectivity is available to the vehicle.

In case PaaK FI receives a Key delivery confirmation after having received a revoke for that key, it shall reissue another key revoke.

No more than one CAK per userID per device shall be generated for the same vehicle. This relationship shall be managed by PaaK FI.

9.1.12 **Keys Status**

###F_PaaK_R_00025### Keys Status

Every logged-in user shall be able to see in the Mobile App the status and names of all issued keys for the corresponding VIN number.

Refer to CAK Management Specification document for more details on Key status values.

9.1.13 Key Revoke

###F_PaaK_R_00026### PaaK Consumer Access Key Revoke

The Key revoke is the action of physically deleting the CAK from storage, such as the BLEM HSM, Android KeyStore, iOS Keychain, or any other system where a copy of the keys might be stored.

The user shall have the ability to revoke the CAKs from the vehicle or the Mobile device.

The user shall be able to revoke only his keys associated with his identity. The user shall be allowed to remove his keys from the device from which the request is made and from other devices. The user shall not be allowed to remove keys that are not associated with his identity either from the same device or from another device.

The user shall be required to enter a security object (PIN, passwd, etc.) upon revoking a key.

To revoke all keys, the user shall use PaaK Reset or Master reset or Brand Reset functionality.

If connectivity of the mobile device to cloud is not available at the time of the revoke, the mobile CAK shall be deleted from the device and the request for key revoke to the cloud shall be queued in the mobile app and delivered later when connectivity becomes available.

If there is an ongoing Bluetooth session between the phone and the vehicle at the time of the key revoke, the Device Session Key (DSK) corresponding to the CAK being revoked shall be revoked from the phone at the same time.

The revoke request to the vehicle shall be delivered to TCU (CGEA) or ECG (FNV2, 3), which shall deliver the command to the BLEM

Key revoke through the vehicle is conditional to the vehicle's TCU connectivity and ECG/TCU power modes. It cannot be delivered to the vehicle through the TCU until TCU establish connectivity with the cloud. The revoke request shall be queued in the cloud and delivered to the vehicle when the vehicle is in coverage or chained with a new key request (refer to Revoke through Mible Device for details on chaining).

The BLEM shall immediately remove the key and its associated BSP code independently of the ignition cycle.

The cloud shall store the key revoke reason, such as user initiated, CRC initiated, PaaK reset, TCU (CGEA) or ECG (FNV2, 3) deauthorized, etc.

The cloud shall notify the Admin users if the revoked key was set as MyKey

Refer to revoke sequence diagram for more details.

###F_PaaK_R_00027### PaaK Consumer Access Key Revoke through Mobile Device

If connectivity of the vehicle to cloud is not available at the time of revoke. PaaK FI shall send a revoke request to the vehicle through mobile devices by chaining the key revoke with a key delivery request response whenever possible.

Upon receiving a key request from any registered device for a particular vehicle, PaaK FI shall check if there are pending revokes for that vehicle and chain them, if any, to the requested key. The mobile app shall then deliver the revoke requests and the new key in the chronological order to the vehicle and send a confirmation back to PaaK FI for each key revoke and delivery separately.

PaaK FI shall then update the keys status accordingly.

###F_PaaK_R_00028### PaaK Consumer Access Key Revoke Process

The process to do a Key Revoke from the Mobile Device shall follow the following steps:

- The user initiates revoke key on the mobile app.
- The mobile app deletes the CAK from the Mobile Device immediately and sends revoke key request to PaaK FI via NG SDN. If mobile app is not in coverage area the request shall be queued.
- PaaK FI validates the revoke key request and request a vehicle revoke request payload encrypted with BLEM SyncP from IVSS
- PaaK FI sends secure payload to the TCU (CGEA) or ECG (FNV2, 3), or through the phone during key delivery (chaining).
- TCU (CGEA) or ECG (FNV2, 3) decrypts and decodes the payload (SYNCP) and sends it to the BLEM
- If the phone gets the chained key revokes it shall send them one by one to the BLEM through BLE
- BLEM decrypts the keys (BLEM SYNCP) and revokes the key and its associated BSP code.
- BLEM sends confirmation that key was revoked to the PaaK FI via the TCU and via the Phone if received from the phone (chaining).
- PaaK FI updates key status. (Key deleted from BLEM and mobile app)
- If revoked key was set as MyKey, Paak FI sends a notification to all admin users notifying them that a Mykey got revoked

###F_PaaK_R_00029### BSP Setup

Once the CAK is delivered to both the Mobile and the Vehicle, the User shall be able to create a BSP code associated with his CAK through SYNC system.

The BSP code shall allow the customer to access and operate the vehicle as a backup method for starting the vehicle and driving away in case the mobile device is not present or run out of battery or any other reason that prevents the BLEM from detecting the mobile device or recognizing the CAK. The user shall also be able to create a valet code assuming BSP is setup.

See BSP Specification document for more details on the backup solution

9.1.14 Phone Change

###F_PaaK_R_00030### Phone Change

When a customer changes his mobile device (phone destroyed, lost, etc.), his mobile Key cannot be reused in the new phone and he shall request a new CAK key for the new device from the cloud.

The customer shall be able to revoke the existing key of the old device from the new device.

9.1.15 Pairing

###F_PaaK_R_00031### Pairing and Bonding for PaaK

The preferred pairing method is “passkey Entry” (with user interaction).

The BLE device that wants to share secure data with the Mobile Device must first pair with each other. The BLE Security Manager Protocol (SMP) carries out the pairing in 3 steps.

- Step 1: The two connected Bluetooth low energy devices announce their input and output capabilities and from that information exchange public keys is to generate the Short Term Key (STK). The devices agree on a Temporary Key (TK) that along with some random numbers creates the STK.
- Step 2: The Peripheral BLE device will send a prompt to the user to pair by entering six digit number, shared on the mobile device app UI, known as the Passkey. Once the Passkey is entered successfully the devices will move to step 3.
- Step 3: The two devices establish a long term connectivity (bonding) by exchanging a long term key (LTK)

Pairing between the mobile device and the BLEM should happen once and the pairing information persisted in both mobile device and the BLEM.

9.1.16 Initial Pairing with Key Delivery

###F_PaaK_R_00032### Initial Pairing with Key delivery between Mobile Device and Vehicle

This connection process shall be completed with limited interaction between the user and a mobile device interface.

Preconditions:
- The vehicle shall be authorized before the pairing can be executed.

The initial pairing of the mobile device happens during the key delivery process, after which the two devices establish a BLE bonding by exchanging a Long Term Key (LTK) as described in section 9.1.17, and will be used for subsequent connections.

The key delivery and pairing shall proceed as follows:

1- BLEM iBeacon shall constantly be advertising in a connectable mode
2- If no key on the phone, the phone detects the beacon but don’t wake-up the app.
3- Upon key request and installation in the mobile device the user has to move close to vehicle with the mobile app in the foreground
4- The mobile app detects the advertising, recognizes the selected vehicle BeaconID and initiates a connection with the BLEM
5- The BLEM initiate a soft Authentication request
6- The mobile device respondes with a soft Autentication response
7- BLEM initiate a BPEK challenge to authorize the mobile device
8- Upon device authorization as a result of the successful challenge, the phone initiates a key delivery and specifies the number of SyncP payloads to deliver (chained key revokes and key delivery)

9- The BLEM request one payload at a time, execute and respond back with success or failure message. The last key delivery package sent from the phone shall be the key associated with the device doing the deliveries
10- for Key delivery message, BLEM verifies the key, and challenges the phone with it.
11- BLEM and the phone are still connected from key delivery session above, BLEM initiates pairing and bonding is completed with Phone).
12- Once pairing and bonding are complete, the BLEM and phone confirm delivery

The mobile app shall notify PaaK FI via the NG SDN that CAK was delivered successfully. The notification shall be queued if mobile device is not connect to the cloud.

The BLEM shall notify PaaK FI through TCU that CAK was delivered successfully.

###F_PaaK_R_00033### BLEM Advertising Trigger

The BLEM shall listen to the authorization message from the TCU (CGEA) or ECG (FNV2, 3), and shall start advertising its iBeacon for key delivery and connection with authorized mobile devices. The BLEM shall allow key delivery while vehicle is in park mode only.

The BLEM shall listen to the de-authorization message from the TCU (CGEA) or ECG (FNV2, 3), and shall stop advertising its iBeacon when the de-authorization message is detected.

9.1.17 Deleting Pairing data

###F_PaaK_R_00034### Deleting Pairing data from Mobile Device

If the mobile device loses its vehicle BLE pairing data (Bluetooth “forget this device”, or network data reset), the BLEM shall try to re-pair with the mobile device.

9.1.18 Beaconing /

###F_PaaK_R_000035### Beaconing and (App Wakeup)

Beaconing is a technology that allows for Beacon region monitoring that uses BLE to detect when user is in the vicinity of Bluetooth Low energy devices that are advertising beacon information.

- In both iOS and Android, the signal advertised by iBeacon and installed in the vehicle shall be used to wake up the Mobile App into the background even if it the app was not running, as per the iBeacon specifications and implementation. Refer to iOS iBeacon specs for exact behaviors.
- The Unique ID of the vehicle’s iBeacon shall be provided to the mobile device during CAK delivery for both Android and iOS to facilitate App wakeup.
- The same ID shall be used by BLEM to advertise non connectable iBeacon and connectable BLE
- The BLEM shall stop advertising when the maximum of 4 devices are connected simultaneously.

9.2 Active / Passive Usage

9.2.1 Active Function Support

###F_PaaK_R_00036### PaaK Active Function Support

PaaK shall enable vehicle Active functionality (RKE functions such as Remote Start, Remote Entry, Remote Frunk unlock, etc.) if the Mobile Device is connected to the vehicle. For a list of all RKE functions supported refer to Appendix 13.6.

The BLEM module shall be able to receive and authenticate a user's requests from 4 authorized mobile devices simultaneously. When the Mobile App has an active authenticated session it shall automatically enable all supported active functions in the Mobile App.

The user shall be able to request any supported Active function by pressing corresponding button in the Mobile app. When more than one vehicle is registered in the mobile app, the user shall be able to select which vehicle he wants to use in his mobile app vehicle garage regardless of internet connectivity status.

###F_PaaK_00037### Determine PaaK RKE Request

The BLEM shall be able to detect multiple authorized mobile devices. In this case if the mobile devices are sending requests simultaneously, the BCM shall handle them from the BLEM in the order of arrival without blocking or ignoring any of the incoming requests.

9.2.2 Ignition States

###F_PaaK_R_00038### Ignition States Starting

The PaaK feature shall be capable of establishing and maintaining a Bluetooth Low Energy connection between the Mobile device and the BLEM in all vehicle Ignition States (Off, Accessory, Run or Crank).

9.2.3 Unlocking the vehicle

###F_PaaK_R_00039### Unlocking the Vehicle

The user shall be able to unlock the vehicle provided the following conditions are met:

- A user request to unlock is received by the vehicle from the Mobile device through the BLE connection (Active Function via BLE)
- The location of an authorized Mobile device meets the Passive Entry range requirements, and the vehicle detects the corresponding door handle has been grabbed or liftgate has been triggered (Passive Function).

9.2.4 Locking the Vehicle

###F_PaaK_R_00040### Locking the Vehicle

The User shall be able to lock the vehicle entry points if the user authenticated Mobile device is not detected in the interior of the vehicle, and the following conditions are met:

- A user request to lock is received by the vehicle from the Mobile device through the BLE connection (Active Function via BLE).
- A user request to lock through the door handle lock button or through the keypad

9.3 Passive Function Support

###F_PaaK_R_00041### PaaK Passive Function Support

PaaK feature shall be required to enable vehicle Passive functionality. If the Mobile Device is connected and authenticated to vehicle, the BLEM shall provide Device location to the BCM to support the following passive functions but not limited to:

- Unlock Driver Door, front right door, rear right door, rear left door, Charge Cord, or Liftgate.
- Lock All
- Welcome mode
- Farewell Mode
- Walk Away Lock

9.3.1 Starting the Vehicle

###F_PaaK_R_00042### PaaK Passive Engine Start

BCM shall start the vehicle under the following conditions:

- An authorized PaaK Mobile device is detected by the BLEM in the interior of the vehicle and within the start range,
- The vehicle gearshifter is in Park and the brake pedal is depressed,
- The vehicle detects that the Push-to-Start button has been pressed.
- The detected device is not disabled by BCM

###F_PaaK_R_00043### PaaK Passive Engine Start Process

Preconditions:

- The BLEM has received the challenge data from BCM
- The BLEM has received a valid challenge response from the mobile device

The Passive Engine Start shall proceed as follows:

- Push to Start Button is pressed.
- Once BCM detects that the Start Button has been pressed, a Passive Start Search Request will be initiated for the interior zone to the BLEM module.
- If BLEM determines there is a Mobile device in the requested search zone based on the localization algorithm,and has a valid challenge response from the Devicethen BLEM will send Crypto Response to the BCM with a Valid search result. If not, then BLEM provides Crypto Response to the BCM and indicates an Invalid search result.
-
- If BLEM does not provide the Crypto Response within some limited time, the BCM treats the search response as Invalid.

9.3.2 Mobile Device and Intelligent Access Key Combination

###F_PaaK_R_00044### Mobile Device and keyfob Combination

If a user with authorized Mobile device and active keyfob is within connection range to the vehicle, the BCM shall detect and prioritize each request from the devices. This decision shall be based on determining the location of each device with respect to vehicle zones and prioritization strategy.

9.3.3 Welcome Mode Standby Time

###F_PaaK_R_00045### Welcome Mode Standby Time

The PaaK feature shall be capable of initiating Welcome Mode based on detection of an authorized Mobile device in the welcome mode zone as long as BCM requests it and BLEM is not in low power mode.

9.3.4 Unlock Pre authentication

###F_PaaK_R_00046### Unlock Pre Authentication

The PaaK feature shall be capable of supporting Device Pre authentication based on detection of an authorized Mobile device in the Passive Entry zone.

Preconditions for Pre-authentication:

- The Approach detection is enabled and requested from BLEM by the BCM
- The Pre-authentication detection is requested from BLEM by the BCM
- BLEM is in Full power mode
- Device is connected and authenticated by the BLEM
- Device is calibrated

The BLEM shall start Pre-Authentication process upon receiving PaakTargetSearchPreAuthZ signal with Value "Enable" from BCM, and shall stop Pre-authentication process upon receiving PaakTargetSearchPreAuthZ signal with "Disable" value or when exiting approach detection.

The BLEM Shall send Device locations for pre-authentication purposes when BLEM is on Full Power mode only. When transitioning to low power modes the BLEM shall stop sending localization messages to BCM, the BLEM shall clear the devices zones information and send invalid for Approach Detection search result.

When Pre-Authentication is enabled, the BLEM shall send search results upon any zone change (driver, passenger, exterior, approach, null) of any of the connected device that is authenticated and authorized.

The BLEM shall localize mobile devices for Pre-Authentication purposes as per existing localization specs defined in section 5.9.6 and in PaaK BLEM SPSS document.

The BCM shall allow passive entry in case a device is pre-autenticated in the corresponding passive entry sub zone requested. If no device is pre-authenticated in the requested sub zone when passive entry happens, the BLEM shall send a search request to the BLEM.

BLEM Power mode shall have priority over pre-authorization, i.e, if the BLEM decides to transition to a low power mode, it shall ignore request from BCM for pre-authentication and invalidate all connected devices states before transitioning to low power mode.

Passive key search shall be higher priority than Approach Detection. If a passive search is received by BCM, the BLEM shall stop all Approach Detection routines and process the new search request

Approach detection is not device specific. However pre-authentication shall be device specific, i.e the BLEM shall report zone changes each time any connected device moves between or outside of the passive entry subzones.

9.3.5 Walk Away Lock

###F_PaaK_R_00047### Walk Away Lock	
10	The PaaK feature shall be capable of initiating Walk away Lock based on detection of an authorized Mobile device leaving the Approach Detection zone, or BCM WAL timer expired after all devices left the vehicle and vehicle doors are closed

Preconditions for Walk Away Lock:
- The Approach detection is enabled and requested from BLEM by the BCM
- BLEM is in Full power mode
- Device is connected and authenticated by the BLEM
- Device is calibrated
- No phone is detected inside the vehicle
- WAL function is activated

BCM shall Lock the vehicle upon receiving an invalid response to the Approach Detection polling from the BLEM

Upon detecting a WAL signal on the CAN Bus, the BLEM shall send a WAL status through BLE channel to the last mobile device that exited the Approach Detection to notify the user that his vehicle was locked.

10.1 PaaK Feature Reset

###F_PaaK_R_00048### Master Reset

Preconditions:

- The SYNC system shall allow Master reset only if the vehicle is in the “RUN mode”. i.e., the ignition status signal is equal to “RUN”,
- The SYNC system shall not allow Master reset if CAK key is configured as a MyKey
- The SYNC system shall not be in a valet mode.

The Master Reset function, initiated via SYNC HMI, shall remove all PaaK rights from the vehicle, with the following results:

- Remove CAK from the vehicle and phone authentication data immediately to prevent any previously authenticated mobile devices from connecting to the vehicle.

- Disable the PaaK feature in the vehicle,
- Cancel Subscription to PaaK feature.
- All mobile devices that had authentication rights prior to execution shall no longer have PaaK capabilities for the vehicle.
- The BLEM shall transmit Key Revoked alert to the TCU (CGEA) or ECG (FNV2, 3) module.
- The TCU (CGEA) or ECG (FNV2, 3) shall deliver the alert to the cloud even if it is in Off state
- Change the TCU (CGEA) or ECG (FNV2, 3) state to waiting for authorization.
- PaaK enrollment is removed from CVFMA

- BSP shall be reset from the BLEM.
- Master Reset shall continue even if BLEM revoke fails.
- BLEM shall retry deleting the keys upon detecting de-authorization state signal from the TCU (CGEA) or ECG (FNV2, 3).

###F_PaaK_R_00049### Master Reset Process

The Master Reset shall proceed as follows:

- The customer Initiates Master Reset via SYNC HMI.
- A first popup will be displayed for Master Reset warning the customer that their keys will be deleted.
- If the customer clicks continue on the first popup, a second popup will be displayed informing the customer that the keys are going to be deleted and prompt the customer if he wants to continue.
- After they click continue on second popup the keys are revoked and the rest of the master reset occurs without another interaction from the customer
- BLEM receives the reset/revoke request and revokes the CAKs and BSP codes, increase the SyncP counter by 1000 and send a SYNCP signed Master Rest Alert through TCU (CGEA) or ECG (FNV2, 3) to the Vehicle SDN.
- Vehicle SDN Sends the BLEM Message to CVFMA for cascade
    - PaaK FI receives the message and logs this removal event – no action taken
    - GVMS receives the message and increments Server Message ID by +3000
- Vehicle SDN receives the TCU (CGEA) or ECG (FNV2, 3) Master Reset Alert, decodes and decrypts itand updates the authorization status to unauthorized for the VIN.
- Vehicle SDN sends an alert to CVFMA to de-enroll the customer.
- CVFMA de-enrolls VIN in PaaK and sends remove subscription alert to Subscription Management to cancel subscription.
- CVFMA notifies PaaK FI of Master Reset alert.
- PaaK FI validates that CAK can be revoked and request an encrypted revoke request from IVSS for each for each CAK associated to the VIN.
- PaaK FI sends revoke notification to Message Center to notify each mobile device affected
- Mobile app receives revoke message with Key ID and revokes the key.
- The Mobile device sends status back to PaaK FI with a revoke confirmation
- PaaK FI shall notify the user that PaaK is not functional due to a master reset on the vehicle

###F_PaaK_R_00050### Brand Reset

Preconditions:

- The SYNC system shall allow Brand reset only if the vehicle is in the “RUN mode”. i.e., the ignition status signal is equal to “RUN”.
- The SYNC system shall not allow Master reset if CAK key is configured as a MyKey.
- The SYNC system shall not be in a valet mode.

The Brand Reset function, initiated via SYNC HMI, shall trigger the removal of all PaaK rights from the vehicle, with the following results:

- BLEM shall delete the keys upon detecting de-authorization state signal from the TCU (CGEA) or ECG (FNV2, 3).

- Remove CAK from the vehicle and phone authentication data immediately to prevent any previously authenticated mobile devices from connecting to the vehicle.
- Disable the PaaK feature in the vehicle,
- Cancel Subscription to PaaK feature.
- All mobile devices that had authentication rights prior to execution shall no longer have PaaK capabilities for the vehicle.
- The BLEM shall transmit Key Revoked alert to the TCU (CGEA) or ECG (FNV2, 3) module.
- The TCU (CGEA) or ECG (FNV2, 3) shall deliver the alert to the cloud even if it is in Off state
- Change the TCU (CGEA) or ECG (FNV2, 3) state to waiting for authorization.
- PaaK enrollment is removed from CVFMA
- BSP shall be reset from the BLEM.

###F_PaaK_R_00051### Brand Reset Process

The Brand Reset shall proceed as follows:

- The customer Initiates Master Reset via SYNC HMI.
- A first popup will be displayed for Brand Reset warning the customer that their keys will be deleted.

- If the customer clicks continue on the first popup, a second popup will be displayed informing the customer that the keys are going to be deleted and prompt the customer if he wants to continue.
- After they click continue on second popup the Brand reset occurs without another interaction from the customer
- Upon detecting de-authorization state signal from the TCU (CGEA) or ECG (FNV2, 3), the BLEM revokes the CAKs and BSP codes, and increase the SyncP counter by 1000 and send a SYNCP signed Alert through TCU (CGEA) or ECG (FNV2, 3) to the Vehicle SDN.
- Vehicle SDN Sends the BLEM Message to CVFMA for cascade
- PaaK FI receives the message and logs this removal event – no action taken
- GVMS receives the message and increments Server Message ID by +3000
- Vehicle SDN receives the TCU (CGEA) or ECG (FNV2, 3) Master Reset Alert, decodes and decrypts itand updates the authorization status to unauthorized for the VIN.
- Vehicle SDN sends an alert to CVFMA to de-enroll the customer.
- CVFMA de-enrolls VIN in PaaK and sends remove subscription alert to Subscription Management to cancel subscription.
- CVFMA notifies PaaK FI of Master Reset alert.
- PaaK FI validates that CAK can be revoked and request an encrypted revoke request from IVSS for each for each CAK associated to the VIN.
- PaaK FI sends revoke notification to Message Center to notify each mobile device affected
- Mobile app receives revoke message with Key ID and revokes the key.
- The Mobile device sends status back to PaaK FI with a revoke confirmation
- PaaK FI shall notify the user that PaaK is not functional due to a master reset on the vehicle

###F_PaaK_R_00052### PaaK Reset

Preconditions:

- SYNC checks a TP CAN message from the BLEM module to determine to display the PaaK reset menu
- SYNC system shall allow PaaK reset only if the vehicle is in the "RUN mode". i.e., the ignition status signal is equal to "RUN".
- The SYNC system shall not allow Master reset if CAK key is configured as a MyKey
- SYNC shall not be in a valet mode.

The PaaK Reset function, initiated via SYNC HMI, shall revoke all CAK and BSP codes from the BLEM and CAK from mobile app. The BLEM shall transmit Key Revoked TP message to the TCU (CGEA) or ECG (FNV2, 3) module.

The TCU (CGEA) or ECG (FNV2, 3) shall deliver the Alert to the cloud even if it the vehicle is turned OFF. Removal of PaaK rights from the vehicle shall immediately prevent any previously authenticated Mobile devices from connecting to the vehicle.

PaaK reset shall not cancel subscription neither un-enroll the user from PaaK and the user shall remain authorized to the vehicle.

BLEM shall report execution result back to SYNC via TCU (CGEA) or ECG (FNV2, 3) and shall send an alert to the cloud with the execution result.

In case of BLEM failure to revoke the keys, PaaK FI shall not revoke keys from the mobile devices

###F_PaaK_R_00053### PaaK Reset Process

The PaaK Reset shall proceed as follows:

- The customer initiates PaaK Feature Reset via SYNC HMI.
- BLEM receives the reset request, removes CAKs and BSP codes and increases the SyncP counter by 1000.
- BLEM then signs and sends revoke key alert to the Vehicle SDN via the TCU (CGEA) or ECG (FNV2, 3).
- TCU (CGEA) or ECG (FNV2, 3) reads the alert and generates a success or fail message to Sync
- Vehicle SDN decrypts the revoke request and sends revoke command to PaaK FI.
- PaaK FI validates that CAK can be revoked and request an encrypted revoke request from IVSS for each for each CAK associated to the VIN.
- PaaK FI sends revoke notification to Message Center to notify each mobile device affected
- Mobile app receives revoke message with Key ID and revokes the key.
- The Mobile device sends status back to PaaK FI with a revoke confirmation

###F_PaaK_R_00054### Vehicle Removal from Customer Account

The user shall have the ability to remove a vehicle from his account from the Mobile App or form Ford self portal through the Web.

The user shall be able to revoke only VINs associated with his account; no other user VIN association for the same VIN shall be allowed to be removed from the phone either from the same device or from other devices
The VIN remove shall result in revoke of the associated CAK from the phone and the CAK and BSP code from the BLEM, and the customer subscription to PaaK removed from subscription management.

The user shall be required to enter a security object in the mobile app (PIN, passwd, etc.) upon requesting a VIN Remove.

The VIN Remove shall also de-enroll the user in CVFMA, and remove the VIN from customer account in CRM.

If the user is the last user authorized in this vehicle, the VIN remove shall clear setting in the TCU (CGEA) or ECG (FNV2, 3) and reset TCU (CGEA) or ECG (FNV2, 3) authorization status back to Waiting Authorization state, and the user subscription to PaaK removed from subscription management. The VIN remove shall be accessible from the mobile app only when connectivity to cloud is available to the mobile device.

The user shall not be allowed to remove a vehicle if the mobile app is not connected to the cloud.

###F_PaaK_R_00055### Vehicle Removal from Customer Account Process

The vehicle removal from customer account shall proceed as follows:

- The Customer removes a vehicle from his account on the mobile app or from the Web.
- If from the Mobile App, The mobile app sends a remove vehicle request to common SDN.
- Vehicle SDN de-authorizes the customer (if already authorized).
- If the user is the last removed authorized user from the Vehicle SDN in previous step:
    - All users shall be de-authorized in the Vehicle SDN and Vehicle SDN shall updates Authorization Status to “Waiting for Auth”.
    - SDN sends Clear user settings command to TCU (CGEA) or ECG (FNV2, 3).
    - TCU (CGEA) or ECG (FNV2, 3) clears the user settings.
    - Vehicle SDN sends command to TCU (CGEA) or ECG (FNV2, 3) to update authorization status.
    - The BLEM will monitor the status of the TCU (CGEA) or ECG (FNV2, 3) and when the TCU/ECG is deauthorized/”Waiting for Auth” then the BLEM will revoke its keys and BSP passcodes then send a revoke alert back to the TCU/ECG.
    - TCU (CGEA) or ECG (FNV2, 3) changes the authorization status to “Waiting for Auth”.
    - TCU (CGEA) or ECG (FNV2, 3) then sends success response to the Vehicle SDN.
    - If TCU (CGEA) or ECG (FNV2, 3) sends failure, Vehicle SDN runs a reconciliation which will re-issue the command again to the TCU / ECG to update the authorization status.
- Vehicle SDN then sends the de-authorize request to the CRM and CRM removes the VIN from the account profile.
- Vehicle SDN sends vehicle authorization change request to CVFMA which de-enroll the user from PaaK.
- CVFMA sends remove subscription alert to Subscription Management which removes the user from the subscription.
- CVFMA sends remove alert to PaaK FI.
- PaaK FI validates that CAK can be revoked and request an encrypted revoke request from IVSS for each CAK associated to the VIN.
- PaaK FI sends revoke notification to Message Center to notify each mobile device affected
- Mobile app receives revoke message with Key ID and revokes the key.
- The Mobile device sends status back to PaaK FI with a revoke confirmation
- PaaK FI sends secure payload to the TCU (CGEA) or ECG (FNV2, 3).
- TCU (CGEA) or ECG (FNV2, 3) decrypts and decodes the payload (SYNCP) and sends it to the BLEM
- BLEM decrypts the keys (BLEM SYNCP) and revokes the key and its associated BSP code.
- BLEM sends confirmation that key was revoked to the PaaK FI via the TCU (CGEA) or ECG (FNV2, 3).
- PaaK FI updates key status. (Key deleted from BLEM and mobile app)

10.2 PaaK Range

10.2.1 PaaK Exterior Passive Entry Range

###F_PaaK_R_00056**### PaaK Exterior Passive Entry Range**

For the PaaK (passive entry) variant, the feature shall recognize an authorized phone as approved for entry if it is located outside the vehicle between 0m and 2.0m from the vehicle exterior (vehicle skin).

10.2.2 Welcome/Farewell Mode Range

###F_PaaK_R_00057**### Welcome / Farewell Mode Range**

The PaaK feature shall respond to Welcome and Farewell Mode feature (if supported by vehicle and not disabled by user), if an authorized Mobile device is detected within approach range of the vehicle, that is 3m from vehicle skin. Welcome mode shall be triggered when IGN is in OFF position only.

The PaaK feature may be unable to respond to Welcome/Farewell Mode if fob-based PEPS Welcome Mode feature is currently disabled in the vehicle, for the following reasons:

- A Fault has been detected in the antenna circuitry
- Reduced power mode of the BLEM

See BCM functional specification document for details.

10.2.3 PaaK Passive Start Range

###F_PaaK_R_00058**### PaaK Passive Start Range**

The PaaK feature shall have a zone inside the vehicle selected as approved for starting the vehicle.
The detection zone shall be vehicle interior zone .

10.2.4 PaaK Passive Start Over Range

###F_PaaK_R_00059**### Passive Start Over-Range**

The PaaK feature shall not recognize an authorized phone as approved for starting the vehicle if it is located more than 20 cm outside of the vehicle’s exterior skin.

Mobile device located outside of the vehicle interior and beyond 20cm shall not be detected for Passive Start function.
Bluetooth Low Energy Antenna Module packaging and the number of antennas must be sufficient to cover vehicle interior zone as defined above.

10.2.5 Connection Range Requirement

###F_PaaK_R_00060**### Connection range**

The vehicle shall be able to connect to an authorized Mobile device(s) located within 40m of the vehicle.

10.2.6 Localization Range Requirement

###F_PaaK_R_00061**### Localization Range**

The vehicle shall recognize an authorized Mobile device as approaching the vehicle, if it is located within 6m of the vehicle.

10.2.7 **PaaK Zones**

###F_PaaK_R_00062### PaaK Zones

PaaK feature shall classify a Mobile device's location per below diagram and table:

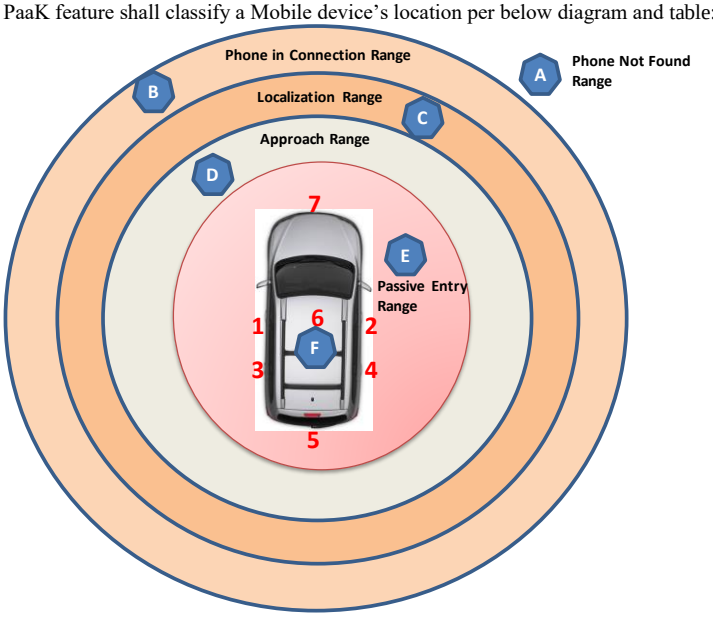


Figure 7 Phone as a Key Classification based on Range to vehicle

Range	Activity
A. No Phone in range	BLE Available
B. Connection range	Active operations (RKE)
C. Localization range	Localization Challenge
D. Approach range	Welcome Light
E. Passive Entry range	
1 Front Left door	Passive entry
2 Front right door	Passive entry
3 Rear Left door	Passive entry
4 Rear Left door	Passive entry
5 Outside Trunk	Passive entry
F. Inside Vehicle	Detection of phone inside/outside
1 Inside Vehicle	Passive Start

Table 16 Ranges vs Activity table

10.3 Mobile App

10.3.1 Mobile App Software Components

###F_PaaK_R_00063### Mobile App Software Components

The mobile application shall be packaged with its required security and connectivity software components provided by suppliers or internally developed. All mobile app software components shall be compliant to Ford approved application/library level obfuscation and code signing solutions.

###F_PaaK_R_00064### Mobile App Installation

The PaaK feature will be part of the owner app that supports the following for installation:

- Mobile App shall meet all standard guidelines for releasing applications in App store and Google Play.
- Mobile App shall be available in App Store in NA, China, Europe and Mexico to install.
- Mobile Device shall have enough space to install the app.
- App notification shall be enabled.
- Device shall be PaaK capable as specified in Device Capability check section.

For more details refer to the Mobile App specs.

10.3.2 Mobile App Uninstallation / Re-installation

###F_PaaK_R_00065### Mobile App Uninstallation / Re-installation

During Mobile App uninstallation:

- Mobile OS shall remove Mobile App data including CAK and VINs.
- The Mobile private key shall be removed and the App unique ID shall not be reused.
- The current vehicle CAK becomes an orphan Key and cannot be automatically revoked from the Vehicle.

After Mobile App re-installation:

- App ID shall be different.
- The User shall request a new CAK in order to be able to use his phone as a key.
- The mobile app shall display the existing keys to the user prior to requesting a new key. The customer will have the opportunity to revoke the orphan key from the vehicle.

10.3.3 Mobile App User Log Out

###F_PaaK_R_00066### Mobile App User Log Out

If a user actively logs out from the mobile application, the application shall not revoke the CAK keys or the Mobile public and private keys.

CAK with its parameters data and the mobile private key shall be preserved upon logout and saved on the mobile device. CAK shall be put in a suspended state that will prevent it from being used when the customer is logged out.

If, at active logout, one or more keys are pending delivery to the vehicle, the mobile app shall notify the user that these keys pending delivery to the vehicle will be deleted.

The mobile app shall be able to access the previous CAKs and Mobile private key and resume normal PaaK functions upon re-login.

- The Cloud shall supply a “salt” value to the app which the app will use to encrypt/decrypt the CAK
- At login the phone shall get the list of salts that correspond to the keys already delivered to that phone for that user.
- At Key request the phone shall get the CAK with its corresponding salt.
- At logout, the “salt” will be deleted from the phone. The encrypted CAK will be kept in the device key store.
- At re-login the mobile app will get the salt from the cloud (PaaK FI) and use it to decrypt and recover the CAK as before.

The mobile application shall be able to access CAKs and any related data and keep normal operations if the user gets passively logged out due to any the following event:

- Backend SW upgrade, SW patch, or server reboot for maintenance, where login session tokens get lost,
- Mobile App upgrade (without uninstall),
- Mobile OS software upgrade,
- Login session time out,
- Session termination due to login to same account from another device
- Any other event that forces the customer to passively logout or lose his login session.

10.3.4 Alternative Connection Support

###F_PaaK_R_00067### Alternative Connection Support

When the BLEM and Mobile Device have an established BLE connection, the Mobile App shall use the BLE connection for the functions shared with Command and Control.
When the mobile is out of BLE range the mobile app should indicate to the user that the commands are not being sent over BLE. The Mobile App shall use the existing Command and Control feature.

###F_PaaK_R_000688### Multiple Connection Manager Support

The mobile application shall be packaged with both connectivity manager configurations, i.e GAP Central and peripheral modes. when the BLEM is in a Central configuration Role the phone should be in the Peripheral Role and vice versa.

The mobile application shall be able to download the BLEM corresponding configuration data from the backend via VCS API upon adding a VIN to the garage to determin which GAP role to apply to this VIN.

The Moble application shall use the corresponding connectivity manager for evey subsequent connection to the BLEM.

10.4 Enhanced Memory Requirement

###F_PaaK_R_00069### PaaK Phone Association/Disassociation to Enhanced Memory Profile

The PaaK Mobile Device shall be associated/disassociated to Enhanced Memory Driver Profile provided the following conditions are met:

- The Vehicle is equipped with Enhanced Memory feature
- Enhanced Memory User Profile Feature set to ON.

- Mobile App Downloaded & Installed; User logged in the Mobile App and it is running in the background.
- Mobile device and vehicle BLEM have active consumer access keys (CAKs).
- The User should have already created a user profile.
- Mobile Device and BLEM paired & connected; Mobile Device is inside the vehicle.

For more details refer to Enhanced Memory Spec.

###F_PaaK_R_00070### Enhanced Memory Profile Recall via PaaK Phone

Enhanced Memory Profile shall be recalled if at least one Mobile Device is associated to User Profile and user initiates the following:

- On RKE request, the BCM identifies the Mobile Device that triggered the request and determines if that Mobile Device has an association to User profile. Based on this determination the User Profile is recalled.
- On Passive Entry Search Request, when the user is approaching the vehicle, the BCM learns the Mobile Device presence and determines if that Mobile Device has an association to User profile. Once the driver door handle is pulled, the user Profile is recalled.

For more details, refer to Enhanced Memory Spec.

10.4.1 MyKey Requirement

###F_PaaK_R_00071### Create/Clear MyKey Phone

The PaaK Mobile Device shall be allowed to be created/cleared as MyKey device provided the following conditions are met:

- MyKey Feature set to ON.
- Mobile App Downloaded & Installed; User logged in the Mobile App and it is running.
- Mobile device and vehicle BLEM have active consumer access keys (CAKs).
- Mobile Device and BLEM paired & connected;
- 1 (One) Admin device (Phone or Key Fob) inside the vehicle.
- Ignition Status is Run &Vehicle Speed is less than 8 KPH.

Every new Phone authorized for PaaK feature shall default to Administrative profile

PaaK Mobile Device association/disassociation shall only be completed through MyKey Feature via Sync interface per below sequence:

- While inside the vehicle, User selects Settings➔ MyKey➔ Create MyKey Phone to setup MyKey menu from Sync.
- Using Mobile App GUI of the Mobile Device to be programmed as MyKey, the user sends RKE Lock command.
- A popup “Key restricted at next start” shall be seen.
- Sync displays the total Admin Key and total MyKey for the vehicle.

To clear MyKey settings User must have at least 1 (one) Admin Device (Phone or Key Fob) inside the vehicle and select "**Clear MyKey Phone"** from Sync. This action shall clear all MyKeys at the same time.

Upon creating or clearing a MyKey, the BLEM shall send amessage to Paak FI to update the Key status accordingly

For more details refer to MyKey Spec.

10.5 Dealer / Service

10.5.1 **Module Replacement**

###F_PaaK_R_00072### BLEM Replacement

Pre-conditions:

- ECG and TCU provisioned ,
- BLEM Supplier feed already ingested in GVMS,

Target ID Transfer process shall be executed between BLEM and BCM. The BLEM module comes locked from the Supplier and the Dealer shall unlock it through Target ID Transfer process. CAKs shall be revoked from the new BLEM when the replacement occurs, and mobile Keys associated with previous BLEM shall be revoked when PaaK FI receives a BLEM provisioning alert.

myKey and Enhanced Memory shall be re-associated manually by the user upon receiving new CAK.
Refer to the steps in F_PaaK_R_00067, F_PaaK_R_00068 for the steps.

BLEM replacement shall not affect authorization state of the TCU (CGEA) or ECG (FNV2, 3). BLEM module re-provision shall occur.

The BLEM Replacement provisioning process is as follows:

- The BLEM module comes locked from the Supplier and the Dealer shall unlock it with its dealer tools.
-
- The BLEM then change its ProvDID to 0x1 (Unprovisioned) after the BLEM detects the TargetID DID has transitioned from Unlocked to Locked state.
- The BLEM then revokes all CAK and and its associated BSP code, and phones authentication info as part of the BLEM initialization diagnostic routine
- The BLEM provisioning starts at the next the ESN TP message delivery to the TCU (CGEA) or ECG (FNV2, 3) and continue in similar way to the initial BLEM provisioning process.

Ford Service and EOL shall adhere to the requirements for BLEM module replacement found in the BLEM-BLEAM SPSS.

###F_PaaK_R_00073### BLEAM Replacement

If BLEAM is replaced, PaaK shall not be impacted.

For more details check BLEM/BLEAM SPSS.

###F_PaaK_R_00074### ECG Replacement

When a TCU (CGEA) or ECG (FNV2, 3) Replacement occurs, the TCU (CGEA) or ECG (FNV2, 3) shall send an Auth_St signal with "NotAuthorized values (0x0).
Upon detecting this signal, the BLEM shall stop advertising and stop scanning.
When the TCU (CGEA) or ECG (FNV2, 3) authorization state transition from NotAuthorize back to "Authorized" state, the BLEM shall resume advertising and scanning.

For more details, check TCU (CGEA) or ECG (FNV2, 3) SPSS

###F_PaaK_R_00075### BCM Replacement

The BLEM and the new BCM must re-authenticate following the BLEM to BCM authentication process found in the BLEM SPSS.

MyKey and Enhanced Memory will have to be re-associated

BLEM and BCM shall go through Target ID Transfer process and there should be no impact on CAK keys.

10.6 Customers Relations Center (CRC)

10.6.1 CRC Support to PaaK

###F_PaaK_R_00076### Call Center Support

The Ford Call Center Representative shall be capable of explaining the processes of requesting or revoking keys to the user so that the customer can successfully complete these processes using their Mobile app.

The user shall be able to request a key revoke for the keys associated to his identity and check key status of the vehicles to which he is authorized by calling the call center. The call center shall check the identity of the customer as defined in the "User Authentication" section before initiating the key revoke or key status process.

The customer shall provide to the call center agent the key name of the key to be revoked, or select a key name from the list retrieved by the call center agent.

The Cloud shall send a message to the customer notifying him of the CRC revoke request

10.6.2 CRC Authentication

###F_PaaK_R_00077 ### User Authentication

CRC shall define a Ford approved method to authenticate a valid user identity.

Refer to CRC process for user authentication details.

10.6.3 Device Calibration

Device calibration is the process by which various smartphones are calibrated for use with Bluetooth Low Energy (BLE) phone-as-a-key (PaaK) passive entry/start (PEPS) systems

the goal of the calibration process for a phone is to determine an average RSSI offset – a value that compensates for the phone's antenna gain and other construction factors, as averaged across common phone postures (e.g., in hand, in front pocket, in back pocket, in purse, etc.), that contribute to the transmission of signals to/from the vehicle, relative to a "golden device" (from which the vehicle's algorithm calibrations are based).
the result of the calibration process is an offset value that is applied to RSSI measurements for each phone within the vehicle-based RSSI measurement system.

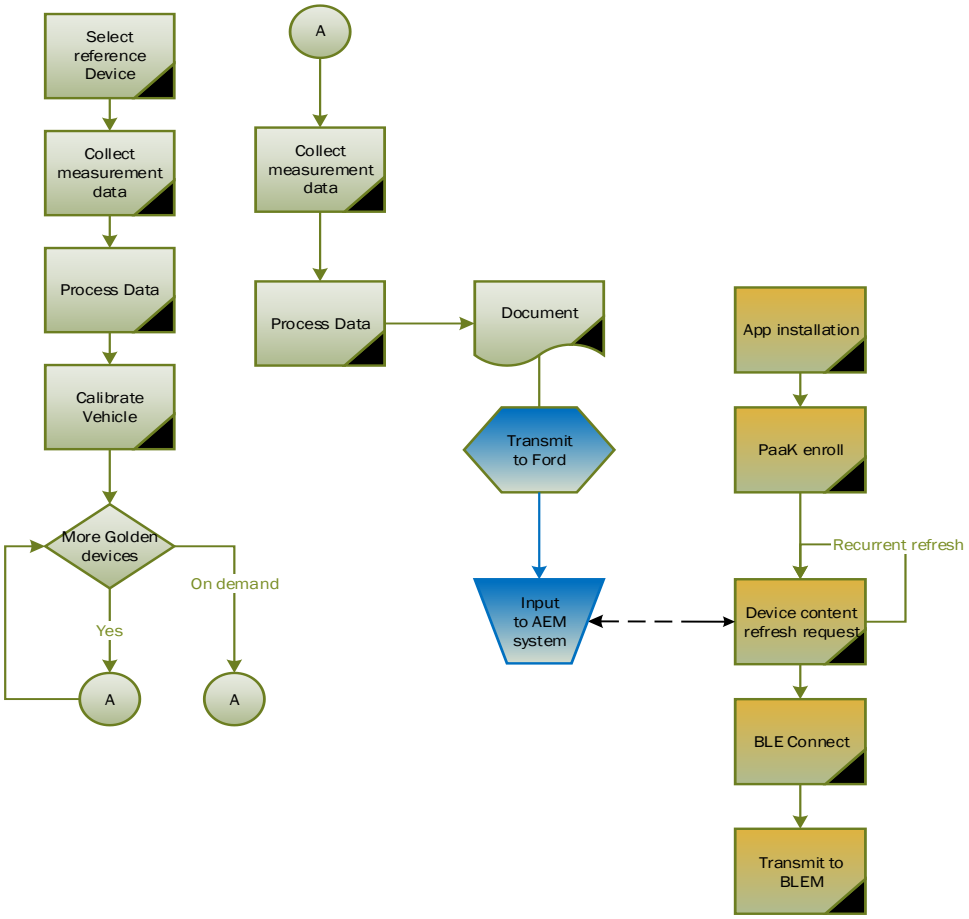


Figure 8 Calibration process diagram

###F_PaaK_R_00078### Reference Device Calibration

- The Reference device shall be the device most commonly used by users at PaaK launch time, most probably an iPhone device. It shall be used to Calibrate the Vehicle localization algorithm.

- The Reference device shall be used to configure the BLEM localization algorithm by determining the accurate RSSI Offset to apply to the localization algorithm in order to align manually measured localization distance with distances automatically calculated by the BLEM algorithm.
- This offset value shall be statically configured and persisted in the BLEM
- This reference offset parameter shall be editable.
- Ford shall communicate to the BLEM supplier which mobilde device to be used as a reference device
- The BLEM supplier shall use the Reference Device to calibrate each vehicle makes and models equipped with PaaK (ECG and FNV2, 3)

###F_PaaK_R_00079### Golden Devices Calibration

- The Golden devices shall be the mobile device list most commonly used by users at PaaK launch time.
- The BLEM supplier shall calibrate each of the golden devices against each vehicle make and model equipped with PaaK, and generate a Calibration Supplier Feed as specified in the next section.
- For each Device and vehicle combination, the BLEM supplier shall generate an RSSI Offset value and a variability indicator value.

###F_PaaK_R_00080### On demand Device Calibration

- On a quarterly basis, ford will request devices calibration for newly introduced devices in the market.
- The BLEM supplier shall calibrate on Ford request each new device introduced in the markets for different regions that Ford considers a supported device.
- BLEM supplier shall also provide Device recalibration of already calibrated devices in the case where calibration errors are identified by Ford or the supplier.
- This device calibration shall follow the same process applied to Golden devices.

###F_PaaK_R_00081### Calibration Supplier Feed

The supplier shall provide a calibration file in a format to be established during the detailed design phase, proposed format to be documented, spreadsheet, xml or Json,

- The supplier shall utilize an existing folder structure in the designated sharepoint site also utilized for supplier software upload, to deliver this file to
- The calibration file shall be signed with the same existing mechanism used to upload supplier software
- The file shall contain version number and creation date, with file name to established during the detailed design phase
- The file shall contain only new calibration data, and no redundant data or previously delivered data

###F_PaaK_R_00082### Device Calibration usage

- The phone shall fetch calibration data (offset,) from the cloud and shall have a mechanism to refresh the data whenever data values change in the cloud

- The phone shall exchange the calibration data wih the BLEM at each session establishement.

- If no calibration data is available fo the device, the app shall provide null values to the BLEM to signal absence of calibration data. The BLEM shall then default to a no calibration data default process for localization purposes, described in the next section.

###F_PaaK_R_00083### No Calibration data default process

If no Data is provided by the connected phone to the BLEM, the BLEM shall:

- Allow Passive Start based on difference between internal and external RSSI signal strength, without relying on the device distance estimation.

- Disable any other Passive Commands for that particular device

###F_PaaK_R_00084### Device Calibration Operations details

TBD

11 NON-FUNCTIONAL REQUIREMENT

The feature PaaK shall meet or exceed user experience expectations and be measured against critical success factors or key performance indicators. Provided below are PaaK operational metrics.

11.1 BLE Requirements

11.1.1 Vehicle BLE Advertising

###NFP_PaaK_R_00001### Vehicle BLE Advertising and scanning

Vehicle shall transmit BLE advertising packets with vehicle identifier at 0.5 – 1.5 second intervals at +5dBm.

The vehicle shall scan for the mobile device for 300ms every 3 seconds.

11.1.2 BLE Connection Range

###NFP_PaaK_R_00002### BLE Connection Range

BLE connection shall be established between user's authorized Mobile device and vehicle within 1 second of Mobile device detecting vehicle advertising packet provided Mobile device and vehicle are within 40m with an unobstructed path.

11.1.3 Authenticated BLE Connection

###NFP_PaaK_R_00003### Authenticated BLE Connection

Authenticated BLE connection shall be established between Mobile device and vehicle within 1 second of unauthenticated BLE connection recognized. Follow security requirements document for implementation details.

11.1.4 PaaK Response Time

###NFP_PaaK_R_00004### Passive Entry Response Time

Vehicle shall complete user triggered request for Passive Entry within 400ms. Mobile device location shall be detected in Outside Vehicle zone prior to allowing user requested action.

###NFP_PaaK_R_00005### Passive Start Response Time

Vehicle shall complete user triggered request for Passive Starting within 250ms. Mobile device location shall be detected in Inside Vehicle zone prior to allowing user requested action. Mobile device estimated location shall be tracked throughout the drive cycle.

###NFP_PaaK_R_00006### Active Commands Response Time

the System shall complete user-triggered request for Active Command within 400ms. This is measured from clicking on the mobile button until receving back an execution status from the vehicle.
Mobile device shall be connected with Vehicle prior to allowing user requested action.

###NFP_PaaK_R_00007### CAK Delivery confirmation through Phone

The CAK shall be delivered to the vehicle and acknowledgement received through the mobile device to PaaK FI in less than **5** second. If there are key revokes chained with the key, each revoke shall not exceed 2 seconds.

###NFP_PaaK_R_00008### CAK installation confirmation

The Vehicle shall provide a key installation acknowledgement through TCU to PaaK FI in less than **1** second

###NFP_PaaK_R_0009### Welcome Mode Activation / Passive Charge Cord Unlock

Welcome mode light and Passive Charge Cord Unlock shall be activated within **300** ms when customer's authenticated Mobile device is located within 3m from the vehicle.

11.1.5 Revoke Response Time

###NFP_PaaK_R_00010### Mobile Device Revoke Time Response

PaaK User shall be able to revoke CAKs for Mobile Device within **1** second.

###NFP_PaaK_R_00011### BLEM Revoke Response Time

BLEM shall remove CAK in less than **1** second.

11.1.6 Cloud Response Times

###NFP_PaaK_R_00012### Cloud Revoke Response Time

The cloud shall push the revoke message to the message center in less than **15** second.

###NFP_PaaK_R_00013### Master Reset / Brand Reset

PaaK User shall be able to initiate Vehicle Master Reset or Brand Reset procedure to remove PaaK Mobile device rights from the vehicle by utilizing the SYNC interface. The vehicle shall remove Mobile device authentication rights from the vehicle BLEM within **30** second of the user completing the Master Reset or Brand Reset procedure in vehicle and display successful removal of the authentication rights via Mobile App interface.

###NFP_PaaK_R_00014### BLEM Provisioning

The cloud shall get a response for a BLEM provisioning in less than **5** minutes

###NFP_PaaK_R_00015### CAK Revoke through Mobile App

The cloud shall get a response for a CAK Revoke in less than **5** second

###NFP_PaaK_R_00016### CAK Revoke through CRC

The cloud shall get a response for a CAK Revoke in less than **5** second

###NFP_PaaK_R_00017### CAK Status

The cloud shall get a response for a CAK Status in less than **5** second

###NFP_PaaK_R_00018### PaaK Reset

The cloud shall get a response for a PaaK Reset in less than 30 second

NFP_PaaK_R_00019### Mean Time between Failures (MTBF)

Based on the fact that there is **730** hours in a month (regular year), and the total downtime for NGSDN currently is **11** hours, and planned downtime is **4** times a month (scheduled maintenance every weekend). PaaK cloud services Mean Time between Failures shall be **180** hours per month.

###NFP_PaaK_R_00020### PaaK Mean Time to Repair (MTTR)

Based on the fact that there is **730** hours in a month (regular year), and the total downtime for NGSDN currently is **11** hours, and planned downtime is **4** times a month (scheduled maintenance every weekend). PaaK cloud services Mean Time to Repair shall be **3** hours

NFP_PaaK_R_00021### PaaK Capacity

The max number of keys to be managed and stored in the cloud for phase 1 shall be **4** keys per car.. Only one CAK shall be allowed per user, per specific device (Mobile App ID) for that user and associated vehicle.

Based on the above assumptions, and for 50,000 vehicles, the total cloud data usage per month is estimate to be **300** MB ingress traffic and 75MB egress traffic. The traffic estimate is less than **1** TPS.

For more details refer to the *Performance and Capacity Requirements*

###NFP_PaaK_R_00022### BLEM Supplier Feed Processing Time

BLEM Supplier Feed process shall be accomplished within 4 hours 99% of the time. (Depends on the BLEM supplier)

###NFP_PaaK_R_00023## BLEM Provisioning Processing Time

BLEM Provisioning process shall be accomplished within 5 minutes 99.9 % of the time

###NFP_PaaK_R_00024### Planned Maintenance Downtime

PaaK Cloud Services maintenance time shall be 11 hours / month or less time. Availability of the cloud shall be 98.5% including planned and unplanned downtime.

Refer to Operational Specs.

###NFP_PaaK_R_00025### PaaK Key Request Time Frame

User shall be able to request a key within 20 seconds (NGSDN/Backend components only)

###NFP_PaaK_R_00026### PaaK Key payload

Size of vehicle CAKs being transferred from device to BLEM shall be between 10-50 KBs.

11.2 Data Retention, Backup and Archival Requirements

Personal information and important data gathered and produced during operations must be stored for a minimum of a year.

11.3 PaaK Event logging

###NFP_PaaK_R_00027### PaaK Event Logging

The mobile app and the BLEM shall generate and capture logging event for CAK management and utilization. Refer to BLEM SPSS, PaaK FI Data Model and Security specs for more details on what event and data format to be captured.

11.4 HMI Requirements

###HMI_PaaK_R_00001### Mobile Device User Interface

The PaaK feature shall provide a user-friendly interface on the Mobile device for accessing all PaaK functions.

###HMI_PaaK_R_00002### No Key Detected Alert

PaaK feature shall alert authorized user through Cluster HMI if the vehicle is currently started and the Mobile device is not detected inside the vehicle, unless an BSP is used in the vehicle.

###HMI_PaaK_R_00003### Command HMI Status Time

Vehicle shall communicate user requested active commands to authenticated Mobile device and display command status/alerts within 1 second of user completing the request on the Mobile device.

###HMI_PaaK_R_00004### PaaK Language Support

PaaK feature shall provide an interface for accessing all PaaK functions and supports the following languages:

- North America: Standard English and French for Lincoln Way and Ford Pass.
- China: Standard English and Simplified Chinese for Lincoln Way and Ford Pass China .
- Mexico: Spanish for Lincoln Way and Ford Pass
- Supported European languages

###HMI_PaaK_R_0005### Bluetooth Indication

When the BLEM and Mobile Device have an established Bluetooth connection, the Mobile App shall have a display to the user showing there is an active Bluetooth connection.

###HMI_PaaK_R_0007### PaaK Usability

PaaK feature shall meet the requirement RQT-002003-022003: Usability of In-Vehicle Systems / Components as defined by Ergonomics in Test Method 00.13-C-1174/4: Procedure for Usability Testing of Components, Systems.

11.5 Security

###NFP_PaaK_R_00030### BLE Secure Connection

The PaaK feature shall provide a secure Bluetooth Low Energy communication channel between the Mobile device and the vehicle, with authentication and encryption implemented at the application layer and in addition to any security provided by the Bluetooth protocol as described in the security specs.

At the Application level, the communication shall be encrypted with a session symmetric key exchanged between the mobile device and the Vehicle using the CAK symmetric key. The session symmetric key shall have a session lifetime and shall not be stored or reused beyond its corresponding session.

11.6 Reliability

###NFP_PaaK_R_00028### PaaK Reliability Requirements

Reliability/durability tests are required to demonstrate that components of the PaaK system will perform its intended functions over the expected service/useful life under all anticipated operating conditions and environments. The tests shall correlate to 95th percentile customer usage as defined by responsible Engineering group. The tests must ensure that expected design and process variations are covered, resulting in adequate product robustness. Test to Failure (TTF) is the preferred test methodology.

- Vehicle Design or Service Life : 10 years / 150,000 miles

PaaK components shall go through pertinent duty cycles as defined in **CETP E-412** document during operational sections of long duration tests such as, High Temperature Endurance, Powered Thermal Cycle, etc. Test to Failure shall be required for new technology or new application for the vehicle program, new supplier, new processes, and high warranty or based on engineering judgement for design robustness. Purpose of Test to Failure shall be to identify any design weaknesses and use the findings to improve reliability and durability of the component.

11.7 System Error Handling Requirements

The PaaK system shall define error states between system interfaces to ensure problems can be detected and remediated properly for the end user. Provided below are error states and messages Ford engineers shall be able to monitor across the PaaK system. For more details refer to section 11.6 Reliability (Functional DTCs).

###NFP_PaaK_R_00029### Functional DTCs

Supplier shall implement Functional Diagnostic Trouble Codes according to components level functional specification document. Refer to ECUs Part 2 doucments of list of PaaK specific DTCs.

11.8 Safety

###NFP_PaaK_R_00030### PaaK Safety Requirement

PaaK feature shall be evaluated agains the Hazard Analysis and Risk Assessment (HARA) assessment in order to comply with the Automotive Integrity Level (ASIL).

All findings shall be document with the appropriate safety engineer and actions should be take to mitigate any identied risk
For more information refer to ISO26262.

###NFP_PaaK_R_00031### PaaK Supplier Feed Availability

BLEM Supplier Feed shall be available 95.6% of the time both with planned and unplanned maintenance times (This might change for BLEM supplier as it has fewer components to configure than ECG)

11.9 Power Management

###NFP_PaaK_R_00032### Transport Mode

PaaK shall not work in transport mode, in order to save battery life during the transportation .

BLEM shall be switched OFF in transportation mode to save power for long-time logistics.

For power management requirements refer to BLEM-BLEAM SPSS.

###NFP_PaaK_R_00033### PaaK Power Modes

The PaaK feature and its components shall provide reliable operation for all Power modes on both Platforms (CGEA and FNV2, 3) as defined in PaaK BLEM SPSS document.

11.10 Operational Requirements

###NFP_PaaK_R_00034### PaaK System Disaster Recovery Requirement

Disaster Recovery shall be captured in IT and Security specs for PaaK.

11.11 Regulatory Requirements

###NFP_PaaK_R_00035### PaaK Regulatory Requirement

BLEM/BLEAM sourced supplier shall ensure compliance to the Federal Motor Vehicle Safety Standards for Theft Protection and Rollaway Prevention (FMVSS 114), Canadian Motor Vehicle Safety Standards for Immobilization Systems (CMVSS14) and GB15740 Protective Devices Against Unauthorized Use of Motor Vehicle requirements for the PaaK system in the markets where the vehicles are sold.

For China market, Bluetooth device needs to pass the SRRC (State Radio Regulation of China) certification. The certification is normally done by Tier1 but it may have some requirements affecting the design, like output power for communication range. Tier1 shall provide more information about the requirements of SRRC for BT device.

11.12 Privacy Requirements

###NFP_PaaK_R_00036### PaaK Privacy Requirement

No known privacy affects for PaaK for launch in U.S., Canada, or China. From a privacy perspective, PaaK will rely on the mobile app for management of the key using the Mobile App ID. Cyber security may want to monitor data points (which may include PaaK-related elements) for suspicious activity, which may need to be disclosed in the mobile app terms.

11.13 User Notification Requirements

###NFP_PaaK_R_00037### PaaK Bluetooth Notification Requirement

User shall be notified by the mobile app if Bluetooth is turned off.

###NFP_PaaK_R_00038### CAK Notification Requirement

User shall get an error message from the mobile app if CAK is not delivered to the Mobile Device.

###NFP_PaaK_R_00039### Out Of Range Notification Requirement

If the vehicle is no longer in the BLE range, the Mobile App shall notify the user and provide an alternative method (cellular) to send Active command when possible.

11.14 Environmental Conditions Requirements

###NFP_PaaK_R_00040### Environmental Conditions Requirements

If environmental conditions, such as rain, heat, or snow are present, the BLEM/BLEAMs shall be able to operate within -40 °C up to 125 °C with an 85% relative humidity.

For further details, please refer to BLEM/BLEAM supplier specification documents.

12 TRACEABILITY REQUIREMENTS

This section is for tracking changes in requirements in the PSD or the other component specs or SPSSs. Traceability is used to track the relationship between each unique product-level requirement and the work products to which that requirement is allocated. Good traceability practices allow for bidirectional traceability, meaning that the traceability chains can be traced in both the forwards and backwards directions. Details will be in the table below once all specs are dropped.

Reqt/Usecase		Requirement Summary	Requirement

Feature Document

PaaK

reference	Section, Paragraph, Requirement #, Use Case #	Description	Type (F) Functional (NF) Non-functional	Function #Function Name
Use Case 3.9	Section 6, UC 3.9	CAK Revoke – Different Mobile Device		
PaaK Reset SD	section 8.1.2	Rest alert is sent to PaaK FI through CVFMA	F	PaaK Reset
Key Name	section 9.1.13	Key unique name is automatically allocated by cloud instead of manually entered by customer	F	CAK Request
Key Request	section 0.1.13	Mobile app should display key status prior to Key Request	F	CAK Request
Device ID	section (.6.2	Device ID is not supported by Cloud. We should rely on Mobile App ID only for Key management	F	Mobile App uninstall
Revoke Response time	Section 10.1.5	Remove requirement on cloud revoke response time for CRC. No achnowlegment is sent back to CRC for CAK revoke.	NF	CRC CAK Revoke
Key detection inside vehicle	section 10.4	Requirement “Mobile Device Inside Vehicle and Lock Request Alert” removed. It is not possible to implement this requirement	F	Mobile Localization
Privacy	section 10.14	PaaK will rely on Mobile App ID instead of on the Device ID for Key management	NF	
Logout	section 9.6.3	The key will be encrypted in the mobile device with a salt provided by the cloud at login or key request, and deleted at logout	F	Logout
Subscription management	section 9.1.3 & 9.9	Update subscription management process and enrollment process	F	Enrollment and Subscription
TCU configuration parameters	section 9.1	Cleanup the list	F	
BLEM provisioning	section 9.1.2	Updated the provisioning process	F	BLEM provisioning
Key Delivery	section 9.1.13	Add BPEK Key details during Key delivery	F	Key delivery
Key delivery confirmation	section 9.1.13	Add details of Key delivery confirmation process	F	Key delivery confirmation
Key Revoke	Section 9.1.15	Add Key Revoke Reason	F	Key revoke
Key Revoke	section 9.1.15	Add Key revoke through Phone scenario	F	Key Revoke through Phone
Logout	section 9.6.3	Added BPEK handling at logout	F	Logout
Initial pairing	section 8.2.1	Renamed section from BLE bonding to Initial pairing with Key delivery. Replaced Sequence diagram that describe the process of key delivery and initial pairing	F	Initial pairing Key delivery
Supplier feed	section 9.1.1	Added iBeacon to the list of parameters	F	Supplier feed
BLEM provisioning process	section 9.1.2	Added retry from cloud in case of failure	F	BLEM Provisioning

Mobile public key	section 9.1.3	Mobile app sent to cloud upon authorization	F	PaaK auto subscribe
Device Capabilitiy check	section 9.1.4	Updated conditions	F	Device Capability check
CAK request	section 9.1.13	Added step up security	F	CAK Request
CAK Delivery	section 9.1.3	Added manual trigger to get the mobile app in foreground	F	CAK Delivery
CAK Revoke	section 9.1.15	Added step up security	F	CAK Revoke
Initial pairing	Section 9.1.18	describe the process of key delivery and initial pairing	F	Initial pairing Key delivery
iBeacon	section 9.1.20	Stope advertising when 4 devices connected	F	Advertising
VIN Remove	section 9.4	Added step up security	F	VIN Remove
Logout	Section 9.6.3	Some clarifications and rewording	F	Mobile app logout
Response times	Section 10.1.4	Added some KPIs	NF	Response times
Cloud response times	Section 10.1.6	Added section 10.1.6 for cloud response times KPI	NF	Response times
VIN Remove	Section 9.4	Clarified CAK remove process	F	VIN Remove
Master Reset	Section 9.4	Clarified Precondition and SYNC user experience	F	Master Reset
PaaK Reset	Section 9.4	Clarified preconditions and CAK revoke conditions	F	PaaK Reset
Device Capability check	Section 9.1.4	Clarified jailbroken/Rooted devices specs	F	Capability Check
V1.4 changes				
Use case	Section 2.1	Change name to auto subscription	F	Auto Subscription
BLEM Provisioning	Section 8.2.6	Update the sequence diagram with Aditional alert and command and additional parameters.	F	BLEM provisioning
BLEM Provisioning	Section 8.2.6	Added a sequence diagram for Off Board BLEM data acquisition and validation	F	BLEM Provisioning
Mobile Public Key validation	Section 9.1.3	Mobile public key shall be validated during authorization phase	F	PaaK Auto subscribe
Feature Reset	Section 9.4	Added counter increase by 1000 for PR and MR	F	Master reset & PaaK Reset
Use Cases	Section 6.3	Added arrows to use cases link, added legend about multiple user icons for organizational purposes	F	General
Use Cases	Section 6.4, 6.5, 6.6	Added reference to DFMEA for all Use Cases exeptions	F	Vehicle, Cloud, Mobile Use Cases
Interface diagram	Section 7	Added links for BLEM orpvisioning and vehicle capability check Updated Interface table	F	Interface diagram.

V1.4.1 changes				
BCM Replacement	Section 9.8.1	Removed impact of BCM replacement on CAK keys	F	BCM Replacement
Eddystone	All sections	Removed reference to Eddystone, iBeacon should be the only one to use	F	All
RKE	Section 1.2	Removed unlock driver door command, kept unlock all instead	F	RKE
FIMCO	All sections	Replaced “FIMCO” with “Target Id Transfer”	F	All
ECUs configurations	Section 9.1	Removed BLEM config and TCU config tables to avoid mismatch and pointed to respective Part 2 docs	F	ECU config params
BLEM provisioning	Section 9.1.2	Removed list of BLEM provisioning parameters, and pointed to the BLEM SPSS doc instead to avoid mismatch	F	BLEM Provisioning
Device Capability	Section 9.1.4	Refered to PaaK phone list document located in the system and testing verification folder for approved devices, to avoid mismatch	F	Device list
Testing support	Section 9.1.7	Removed requirement for providing BLE trace logs from BLEM	F	Logging
Master Reset	Section 9.4	Removed requirement for BLEM to retry 3 times if revoke fails	F	Master Reset
Active command	Section 10.1.3	Clarified NFP_PaaK_R_00006 spec for response time	NF	Response time
Degradation mode	Section 10.1.6	Removed Degradation Mode	NF	Degradation modes
Supported device list	Section 12.1	Removed iPhone, Android and China supported device lists	F	Supported devices
Calibration Data	Section 9.9.3	Added section for Device Calibration Data	F	Calibration Data
Key Delivery	Section 9.1.11	Clarified Key delivery for known devices	F	Key Delivery

Table 17 Tracability table

13 APPENDICES

13.1 Signals List

Signal Name	Reference
PaaKCtlActv_D_Rq	Signal to inform BCM function that it has received a phone request for vehicle action to be performed (remote request).
PaaKCtlActv_Data_No_Actl	Encrypted calculated authentication response data to authorize a request to perform an RKE function from PaaK control function.
PaaKCtlPssv_Data_No_Actl	Encrypted data to authenticate a passive search result from PaaK control function. It is also used in PaaK TargetID transfer. The meaning of the contents of this signal depends on PaaKCtlData_D_Stat, PaaKCtlType_D_Stat.
PaaKCtlType_D_Stat	Signal is used by BLEM function to indicate whether a valid phone has been found by the PaaK control function during the search.
PaaKCtlData_D_Stat	Signal is used by BLEM function to indicate the type of information being transmitted.
PaaKCtlRollCode_No_Stat	Signal is transmitted by PaaK Control function used to align a search from the PaaK Target function with the corresponding search result coming from the PaaK Control function.
PaaKCtlRollCode_No_Copy	Signal represents second copy of the RollCode to ensure alignment of the PaaK found data with the search result data.
PaaKCtlActv_No_Actl	Signal indicates which phone was used to request an RKE function via the PaaK control function (RKE SubID).

PaaKCtlIndx1_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx2_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx3_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx4_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx5_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx6_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx7_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKCtlIndx8_No_Actl	Represents a signal to indicate 1 of up to 63 phones that can be assigned to PaaK Control function. Up to 8 phones can be identified for a given search.
PaaKSerial_D_Rq	Signal represents a request for the BLEM's ESN.
PaaKWakeupActv_B_Rq	Wakeup signal for phone as a key (PaaK) feature from TCU Deprecated as per Rabindra Basak. Not used.

Signal Name	**Reference**
PaaKTrgtType_D_Rq	Signal used by BCM function to indicate what type of search is being requested of the PaaK control function.
PaaKTrgtZone_D_Rq	Signal used by BCM function to indicate what zone in or around the vehicle to be searched by the PaaK control function when a search request is initiated.
PaaKTrgtData_D_Rq	Signal is used by BCM control function to indicate the type of information being shared with BLEM function (sharing of TargetID (secret key)).
PaaKTrgtActvData_No_Rq	Signal contains encrypted challenge data sent by PaaK target function to be used to calculate an authentication response to authorize and RKE function request.
PaaKTrgtPssvData_No_Rq	Signal contains encrypted data along with PaaK TargetID. Contents of the signal has different meaning depending on the *PaaKTrgtData_D_Rq*, *PaaKTrgtType_D_Rq*.

PaaKTrgtRollCode_No_Rq	Signal is transmitted by PaaK Target function used to align a search request from the PaaK Target function with the corresponding search result coming from the PaaK Control function.
PaakESN_St	TP message to provide provisioning data and key status
PaakInfo_Rq	TP message from TCU/ECG with revoke request
PaakInfo_Rsp	TP message from BLEM containing information about the key activity or in response to PaakInfo_Rq
FactoryReset_Rq	Master reset signal
PaakCnnct_D_Stat	BLE Connection status
PaakAddErase_D_Rq	Used to inform BCM that a CAK has been added or removed. Also sends phone index value in PaakAddEraseIndx_No_Rq
PaakAddErase_D_Stat	Feedback to PaakAddErase_D_Rq
PaakAddEraseIndx_No_Rq	Phone Index used with PaakAddErase_D_Rq
	– Feedback to PaakAddEraseIndx_No_Rq
EmbeddedModemReset_Rq	Paak and Brand reset request signal
PaakCtlIndx1_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx2_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx3_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx4_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx5_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx6_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx7_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakCtlIndx8_D_Stat	Signal to indicate Zone localization corresponding to the Indexed device. Up to 8 phones can be localized for a given search
PaakTrgtPreAuthrz_B_Rq	Signal To enable/disable Pre_authentication function

Table 18 Signals List

13.2 Keyless Entry Command List

Fob Button(s)	Activation Description	Mobile App Activation	Result
Panic button	Single Press	TBD	Activate/deactivate panic alarm
	Two presses within 3 seconds	TBD	Activate panic alarm- single press deactivates
Lock button	Single Press	TBD	Lock all doors and liftgates and cancel any global open/close Mark an event for global close.

			Mark even for Remote Start.
	Press and hold for a minimum of 2 seconds	TBD	Global Close request (close all windows and moon roof)
Unlock button	Single Press	TBD	Unlock driver's door and cancel any global open/close Mark an event for global open
	Press within 3 seconds of previous Unlock press	TBD	Unlock all doors and liftgate/trunk
	Unlock Button Press followed by a second unlock button press and hold (for 3 seconds). This whole process must be completed within 10 seconds of the first unlock button press	TBD	Global Open request (open all windows and moon roof)
Lock & Unlock buttons simultaneously	Press and hold for a minimum of 4 seconds	TBD	Toggle one stage and two stage unlocking mode
Trunk Release button	Single Press	TBD	Enable Decklid Switch (for 45 sec (Europe) and no action (NA))
	Two presses within 3 seconds	TBD	Open trunk
Glass Release button	Single Press	TBD	Enable Liftgate Glass (for 45 sec (Europe) and no action (NA))
	Two presses within 3 seconds	TBD	Open liftgate glass
Power Decklid button	Single Press	TBD	Enable Power Decklid Switch
	Two presses within 3 seconds	TBD	Operate power Decklid
Power Liftgate button	Single Press	TBD	Enable Power liftgate (for 45 se (Europe) and no action (NA))
	Two presses within 3 seconds	TBD	Operate Power liftgate (for Europe and NA) and inhibit intrusion and inclination sensing
Manual Liftgate	Single Press	TBD	Enable Exterior Liftgate Switch (for 45 sec (Europe) and no action (NA)) and inhibit intrusion and inclination sensing
	Double Press	TBD	**For Europe:** a) If the latch operation is Unlock only: It enables the exterior switch for 45s and inhibits intrusion/inclination sensing b) If the Latch operation is Release type: It releases the Liftgate, enables the exterior switch and inhibits intrusion/inclination sensing **For NA:** a) If the Latch operation in Unlock only: It enables the exterior switch and inhibits intrusion/inclination sensing. b) If the Latch operation is Release type: It releases the Liftgate,

			enables the exterior switch and inhibits intrusion/inclination sensing.
Right Sliding Door button	Two presses within 3 seconds	TBD	Operate right sliding door
Left Sliding Door button	Two presses within 3 seconds	TBD	Operate left sliding door
Remote Start button	Along with Lock button press, Two presses within 3 seconds	TBD	Initiate Remote Start Request
	Another Single press of the Remote Start button after start	TBD	Will stop Remote Start Operation.

Table 19 Command List

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF DIAGRAMS