Function Group Spec

Center Stack Display System

Custom Scope

Document Type	**Function Specification**	
Template Version	**6.0**	
SysML Report Template Version	**M (4/16/2019)**	
Document ID	**2021-09-20**	
Document Location		
Document Owner	**Aaron Bonnell-Kangas (abonnel1)** **Aaron DeLong (adelong2)** **Eugene Karpinsky (ekarpins)** **Farhan Ehsan (fehsan2)** **Jonathon Wolf (jwolf53)** **Reinaldo Sepulveda (rsepulv6)**	
Document Revision	**FGS0**	
Document Status	**Released**	
Date Issued	**2020-05-22**	
Date Revised	**2021-09-20**	
Document Classification	GIS1 Item Number: **27.60/35** GIS2 Classification: **Confidential**	

Document Approval			
Name	Role	Email Confirmation	Date

Auto-Generated by MagicDraw
Printed Copies are Uncontrolled

DISCLAIMER

This document contains Ford Motor Company Confidential information. Disclosure of the information contained in any portion of this document is not permitted without the expressed, written consent of a duly authorized representative of Ford Motor Company, Dearborn, Michigan, U.S.A.

Copyright, © 2021 Ford Motor Company

This document contains information developed and accumulated by and for FORD MOTOR COMPANY. As such, it is a proprietary document, which, if disseminated to unauthorized persons, would provide others with restricted information, data, or procedures not otherwise available, exposing the FORD MOTOR COMPANY to potential harm.

Employees and suppliers having custody of this specification or authorized to use it must be cognizant of its proprietary nature and ensure that the information herein is not made available to unauthorized persons.

FORD MOTOR COMPANY reserves the right to protect this work as an unpublished copyrighted work in the event of an inadvertent or deliberate unauthorized publication. FORD MOTOR COMPANY also reserves its rights under copyright laws to protect this work as a published work.

This document or portions thereof shall not be distributed outside FORD MOTOR COMPANY without prior written consent. Refer all questions concerning disclosure to the author(s) or to any duly authorized representative of Ford Motor Company.

CONTENTS

Disclaimer 2
Contents 3
1 Introduction 5
1.1 Document Purpose 5
1.2 Document Audience 5
1.2.1 Stakeholder List 5
1.3 Document Organization 8
1.3.1 Document Context 8
1.3.2 Document Structure 9
1.4 Document Conventions 9
1.4.1 Terminology 9
1.4.2 Requirements Templates 9
2 Logical Architecture 10
2.1 Structure 10
2.2 Logical Architecture 10
3 Function Group Description 12
3.1 Logical System Behavior 12
3.1.1 HMI Screens 13
3.1.2 HMI requirements 15
3.2 Logical System Properties 27
3.3 Logical System Requirements 27
4 Function Specifications 30
4.1 Add NFC key InnerSTM 31
4.1.1 Add NFC key InnerSTM Screens 32
4.1.2 Add NFC key InnerSTM requirements 32
4.2 MyKey Management Inner STM 38
4.2.1 MyKey Management Inner STM Screens 38
4.2.2 MyKey Management Inner STM requirements 39
4.3 Personal Profiles Linking STM 41
4.3.1 Personal Profiles Linking STM Screens 41
4.3.2 Personal Profiles Linking STM requirements 42
4.4 Remove NFC Key Inner STM 45
4.4.1 Remove NFC Key Inner STM Screens 46
4.4.2 Remove NFC Key Inner STM requirements 46
5 Revision History 50
6 Appendix 52
6.1 Data Dictionary 52
6.1.1 Logical Messages 52
6.1.2 Logical Parameters 73
6.1.3 Logical Data Types (encodings) 73
6.1.4 Technical Signals 97
6.1.5 Technical Parameters 111
6.2 Glossary 111
6.2.1 Definitions 111
6.2.2 Abbreviations 111

List of Figures

Figure 1: NFC Logical Domain Structure 10
Figure 2: NFC Logical Architecture 11
Figure 3: HMI 12
Figure 4: Add NFC key InnerSTM 31
Figure 5: MyKey Management Inner STM 38
Figure 6: Personal Profiles Linking STM 41
Figure 7: Remove NFC Key Inner STM 45

List of Tables

Table 1: Operation Modes and States on HMI 15
Table 2: Operation Modes and States on Add NFC key InnerSTM 32

Table 3: Operation Modes and States on MyKey Management Inner STM 39
Table 4: Operation Modes and States on Personal Profiles Linking STM 42
Table 5: Operation Modes and States on Remove NFC Key Inner STM..... 46
Table 6: Definitions used in this document..... 111

1 INTRODUCTION

1.1 Document Purpose

The Function (Group) Specification (FS) specifies an individual function / a group of functions.

To get more information about the concept of feature, function and component level abstraction refer to the Ford RE Wiki.

1.2 Document Audience

The FS is authored by the owners of the individual functions. All Stakeholders, i.e., all people who have a valid interest in the functions and their behavior should read and, if possible, review the FS. It needs to be guaranteed, that all stakeholders have access to the currently valid version of the FS.

1.2.1 Stakeholder List

For the latest list of the feature stakeholder and their roles & responsibilities refer to https://www.vsemweb.ford.com/tc/launchapp?-attach=true&-s=226TCSession&-o=iKZxDO0dx3NrTD&servername=Production_Server.

Name	CDSID	Role	Orginization	Stakeholder Group
Reinaldo Sepulveda	rsepulv6	Core Feature Owner	PD, Sys. Eng., Distributed Feat.	Production Design Lead and Feature Owner
Jonathon Wolf	jwolf53	Core Feature Owner	PD, Sys. Eng., Distributed Feat.	Production Design Lead and Feature Owner
Rita Trupiano	mtrupia1	Feature Owner Supervisor	PD, Sys. Eng., Distributed Feat.	Feature Owner Supervisor
Aaron Bonnell-Kangas	abonnel1	Core Feature Owner	PD, Sys. Eng., Distributed Feat.	Production Design Lead and Feature Owner
Eugene Karpinsky	ekarpins	Core Feature Owner	PD, Sys. Eng., Distributed Feat.	Production Design Lead and Feature Owner
Farhan Ehsan	fehsan2	Core Feature Owner	PD, Sys. Eng., Distributed Feat.	Production Design Lead and Feature Owner
Michael Martinez	mmart664	Product Manager	PD, Mobility	Ford Mobile App Design
Matthew Borrelli	mborrel4	Infotainment Systems Engineer	PD, In-Vehicle Infotainment & Connectivity	Infotainment System Design
Iqbal Faheem Sayyed	isayyed	SYNC Technical Program Manager	PD, In-Vehicle Infotainment & Connectivity	SYNC Technical Program Manager
Gail Cheng	gcheng	Infotainment Systems Supervisor	PD, In-Vehicle Infotainment & Connectivity	Infotainment System Design Supervisor
Scott Watkins	swatkins	DI Technical Expert	PD, In-Vehicle Infotainment & Connectivity	Driver Information Design Support
Laura Check	lburek	SYNC Supervisor	PD, In-Vehicle Infotainment & Connectivity	SYNC System Supervisor
Jeffrey Hamel	jhamel7	Product Owner, TPM	PD, Enterprise Connectivity	Ford Mobile App Design

Nhi Torres	ntorres5	Supervisor	PD, EESE, Netcom Diag.	Electrical Architecture Consult
Eric Paton	epaton	Engineer	PD, EESE, Netcom Diag.	Electrical Architecture Consult
Bruce Williams	bwilli28	Product Design Engineer	PD, EESE, Netcom Core	Electrical Architecture Consult
Ankita Vyas	avyas8	Functional Safety Engineer	PD, EESE, Functional Safety	Functional Safety Consult
Nisha Patel	npate152	Core NFC Engineer	PD, EESE, Body & Security Elec.	NFC System Owner
Suthagaran Nagarasa	snagaras	Core NFC Engineer	PD, EESE, Body & Security Elec.	NFC System Owner
Matt Swis	mswis	Core Security & RF Supervisor	PD, EESE, Body & Security Elec.	NFC System Owner Supervisor
David Hernandez	dhern138	Core NFC Engineer	PD, EESE, Body & Security Elec.	NFC System Owner
Akshita Kulkarni	akulka2	Design Engineer, BCM Software	PD, EESE, Body & DAT SW	Software Design
John Ricks	jricks7	Software Supervisor	PD, EESE, Body & DAT SW	Software Supervisor
John Popovecz	jpopovec	Body Module SW Supervisor	PD, EESE, Body & DAT SW	Body Module SW Supervisor
Ahmad Sabri	asabri3	PD Engineer	PD, EESE, Body & DAT SW	Software Design
Andrew Hall	ahall185	Design Engineer, BCM Software	PD, EESE, Body & DAT SW	Software Design
Hosam Irsheid	hirsheid	Software Engineer	PD, EESE, Body & DAT SW	Software Design
Eric Reed	ereed2	VSC SW Engineer	PD, EESE, Body & DAT SW	Software Design
Sam Mehdi	hmehdi	Product Design Engineer	PD, EESE, Body & DAT SW	Software Design
Jeff Lossing	jlossing	Software Engineer	PD, EESE, Body & DAT SW	Software Design
Kevin Hille	khille	Technical Specialist – Immob.	PD, EESE, Body & DAT SW	NFC Immobilizer Function Owner, Design Support
Sachin Magar	smagar	Design Engineer, BCM Software	PD, EESE, Body & DAT SW	Software Design
Adithya Ramachandran	aramac11	Software Engineer	PD, EESE, Body & DAT SW	Software Design

S Bagga	sbagga11	Software Engineer	PD, EESE, Body & DAT SW	Software Design
Vishala Pasala	vpasala	Software Engineer	PD, EESE, Body & DAT SW	Software Design
Maeen Mawari	mmawari	MBSE Engineer	PD, EESE, Body & DAT SW	Software Design
Jim Lawlis	jlawlis	Technical Specialist - Netcom	PD, EESE, Advanced Netcom	Electrical Architecture Consult
Mack Dobbie	mdobbie	HMI Designer	PD, CIED	HMI Support
Patrick Brautigan	pbrautig	UX Engineer	PD, CIED	UX Support
Stavros Dionyssopoulos	sdionyss	DI HMI Engineer	PD, CIED	Driver Information HMI Support
Nicholas Davio	ndavio	HMI Supervisor	PD, CIED	HMI Support Supervisor
Montana Pruett	mpruett2	I&E Engineer	PD, CIED	I&E Support
Uwe Zank	uzank	Supervisor, Security Electronics	PD Europe, Underbody EESE	Security Design Consult
Ahmet Cinar	acinar1	Tech. Expert – Closure Electronics	PD Europe, Underbody EESE	Closure Design Consult
Denney Vellaramkalayil	dvellara	System Engineer, Locking Application	PD Europe, Underbody EESE	Locking Design Support
Jennifer Oak	joak	Connected Marketing Manager	MS&S, US Marketing	Project Champion – Retail
Timothy Son Hing	tsonhin1	Marketing Manager	MS&S, US Marketing	Project Champion – Retail
Mustapha Elkhatib	melkhat1	Product Manager	IT, Mobility, FCS	Fleet Infrastructure Design Support
Michelle Moody	mmoody1	Director	IT, Mobility, FCS	Project Champion – Fleet
Geoffrey Scofield	gscofiel	Product Engineer	IT, Mobility, FCS	Fleet Infrastructure Design Support
Robert Johnson	rjohns75	Product Marketing Manager	IT, Mobility, FCS	Project Champion – Fleet
Yona Shaposhnik	yshaposh	Solution Architect	IT, MPS, Mobility Arch.	Backend Infrastructure Design Support
Jochen Schubert	jschub1	Cybersecurity Engineer	IT, Cybersecurity	Cybersecurity Design Support
Mike Westra	mwestra	Technical Leader – Security	IT, Cybersecurity	Cybersecurity Consult
Simon Hurr	shurr	Security Application Specialist	IT, Cybersecurity	Cybersecurity Consult

Xin Ye	xye7	Technical Specialist - Security	IT, Cybersecurity	Cybersecurity Consult
Jacob Nelson	jnels148	Cybersecurity Engineer	IT, Cybersecurity	Cybersecurity Design Support
Dan Zajac	dzajac8	Cybersecurity Supervisor	IT, Cybersecurity	Cybersecurity Supervisor
Mike Simons	msimon78	Systems Engineer	IT, CVP&P, PaaK	Off Board Function Owner Lead
Steve Craig	scraig33	Technical Program Manager	IT, CVP&P, Integration	Backend Infrastructure Design Support
Faten Fawaz	ffawaz	Basic Design Architect	IT, CVP&P, Basic Design	Backend Infrastructure Design Lead
Henry Popow	hpopow	Quality Engineer	EESE Quality	Quality Coach
Gerard Szczepaniak	gszczepa	Quality Engineer	EESE Quality	Quality Coach
Christina Bloxsom	cbloxsom	Subject Matter Expert	Adv. Policy, SE&SE, ASO	Safety & Regulations Consult
Vivek Elangovan	velango5	Research Engineer	Adv. Feat. Development, RA&E,	Design Support
Aaron DeLong	adelong2	Research Engineer	Adv. Feat. Development, RA&E,	Research Design Lead
John Van Wiemeersch	jvanviem	Supervisor	Adv. Feat. Development, RA&E,	Design Support

1.3 Document Organization

1.3.1 Document Context

Refer to the Specification Structure page in the Ford RE Wiki to understand how the FS relates to other Ford Requirements Documents and Specifications.

1.3.2 Document Structure

The structure of this document is explained below:

Section 1 – Introduction how to use this document including responsibilities and requisite documents. Explains the tterminology. Gives a clarification of the definitions, concepts and abbreviations used in the document.

Section 2 – Function Group Description. Gives an overview and the purpose of the function group.

Section 3 – Functional Architecture: Specifies the overall functional architecture of the function group

Section 4 – Function Specifications: Specifies the logical functions of the function group in detail

Section 5 – List of Open Concerns

Section 6 Revision history including a list of new or modified requirements. The requirements in this document are tagged, and this section contains different types of tables listing all, new, or changed requirements by their title and page no.

Section 7 – Appendix: Presenting additional data mainly in a tabular form, e.g., a data dictionary

1.4 Document Conventions

1.4.1 Terminology

When referring to aspects of the system design, this document uses standardized language to avoid ambiguity and confusion. The following terms are of particular relevance to this document:

Term	Definition
Configuration parameter	A property of a system that is stored in nonvolatile memory and not expected to be changed during system operation. Examples include assigned serial numbers that are unique to each module and static.
Runtime variable	A property of a system that can be read and modified during normal system operation. The variable might be stored in volatile or nonvolatile memory. Examples include stored/saved records, system states, and measured values.
Message	A message defines a data structure whose elements are all transmitted simultaneously. The message might be transmitted within a single system, or across a network between two separate systems. The term “message” is used here to reduce confusion when discussing automotive system behaviors. As it is used in this document, a “message” is identical to the concept of a “signal” as defined in UML/SysML. A message may or may not contain *signals* – see below.
Signal	A signal is a single data element within a message. A signal cannot be transmitted independently of a message, but a message can be transmitted without any signals. As it is used in this document, a signal corresponds to the UML/SysML concept of a *property*.

1.4.2 Requirements Templates

Each requirement, use case or scenario in this specification shall follow the corresponding template given in the document template *Specification_Macros.dotm* at RE Wiki - Specification Templates.

1.4.2.1 Identification of Requirements

1.4.2.2 Requirements Attributes

The templates provided by *Specification_Macros.dotm* define a list of attributes for each requirement. This helps to classify the requirement. The attributes are explained at RE Wiki - Requirements Attributes.

2 LOGICAL ARCHITECTURE

The NFC Entry and Starting feature is designed assuming the following system structure. The components shown are the logical systems; they may map one-to-one onto a physical module, or one physical module might house multiple logical systems.

2.1 Structure

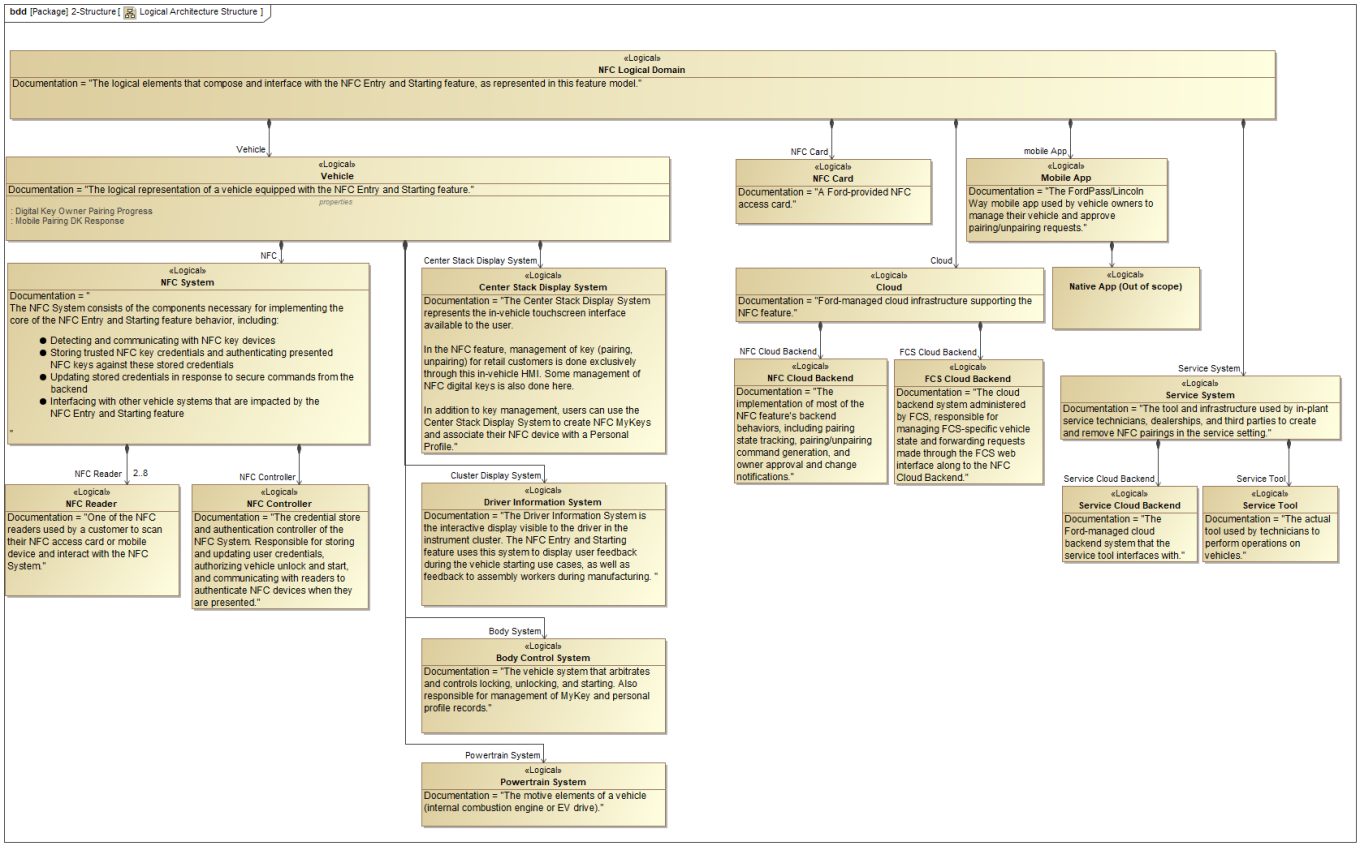


Figure 1: NFC Logical Domain Structure

2.2 Logical Architecture

The Logical Architecture diagram shows the messages that flow between different elements of the NFC Logical Domain. Details on the contents of the messages shown here can be found in the Data Dictionary provided as an appendix.

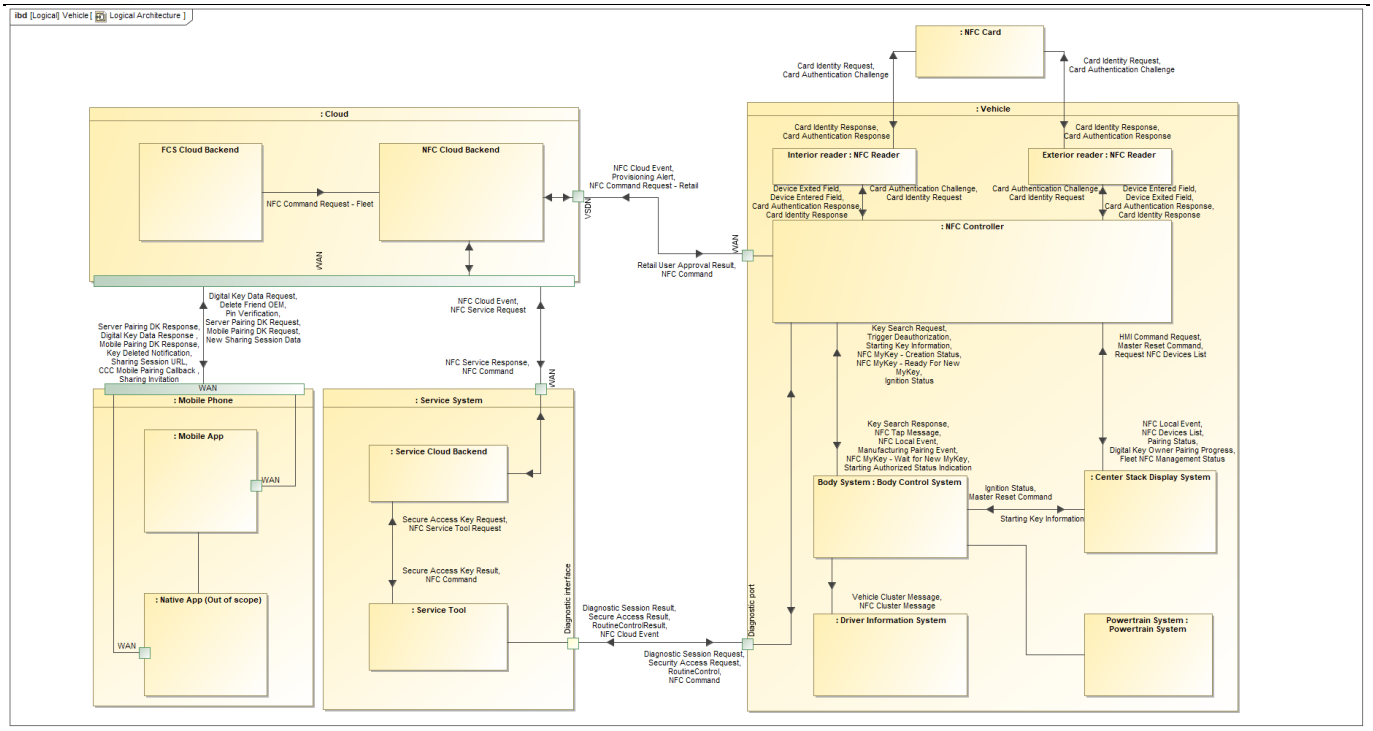


Figure 2: NFC Logical Architecture

3 FUNCTION GROUP DESCRIPTION

This specification consists of documentation about the logical system component **Center Stack Display System.**
The Center Stack Display System represents the in-vehicle touchscreen interface available to the user.

In the NFC feature, management of key (pairing, unpairing) for retail customers is done exclusively through this in-vehicle HMI. Some management of NFC digital keys is also done here.

In addition to key management, users can use the Center Stack Display System to create NFC MyKeys and associate their NFC device with a Personal Profile.

3.1 Logical System Behavior

The screens and flows of the in-vehicle display system that are relevant to the NFC Entry and Starting feature.

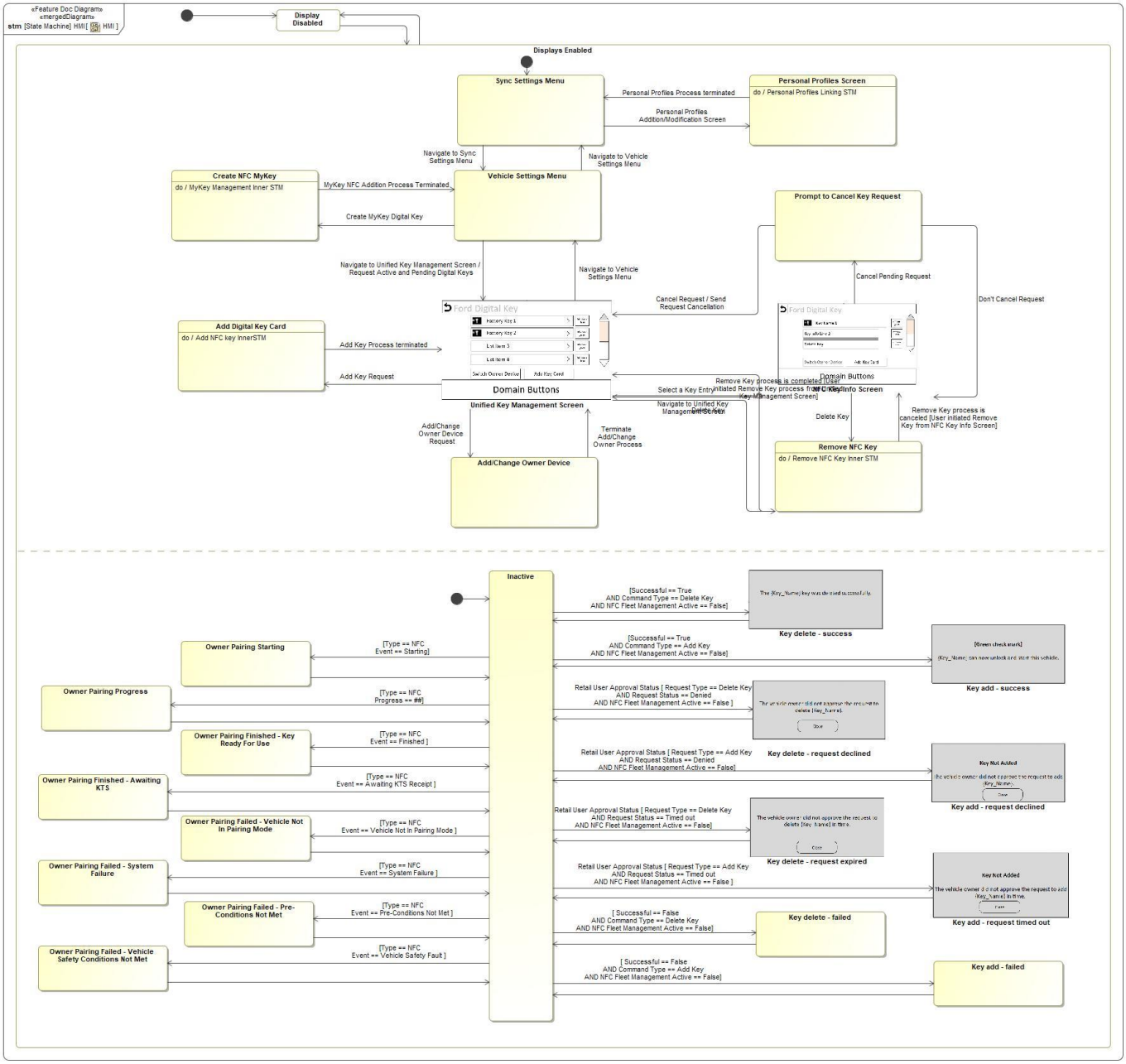


Figure 3: HMI

3.1.1 HMI Screens

State	Description	Requirements Reference
Add Digital Key Card	The screens that allow a user to request pairing of a new NFC access card. Do behavior: Add NFC key InnerSTM	Prompt Screen: No MyKey can pair/change owner device
Add/Change Owner Device	The screens that allow the user to add or change the vehicle's paired owner device.	Prompt Screen: No MyKey can pair/change owner device Prompt Screen: Add Owner Device Prompt Screen: Change Owner Device
Create NFC MyKey	The screens that allow the user to make an NFC device into a MyKey. Do behavior: MyKey Management Inner STM	Enable NFC MyKey Softbuttons
Display Disabled	This state is when the display is disabled and not available for use.	
Displays Enabled	This state is when the display is enabled and available for use by the user.	
Inactive	No pop-up message is being displayed on the screen.	
Key add - failed	Pop-up message informing the user that a key add request has failed to complete for some reason, even though it was approved by the vehicle admin (or did not require approval in the first place). Applicable to retail experience only.	NFC key management notifications - no notifications if vehicle is managed by fleet Show pop-up on key add failure Key add failure pop-up verbiage
Key add - request declined	Pop-up message informing the user that a key pairing request has been denied by the vehicle admin. Applicable to retail experience only.	Content of key add request denial pop-up Show pop-up on key add request denial NFC key management notifications - no notifications if vehicle is managed by fleet
Key add - request timed out	Pop-up message informing the user that a key add request has expired because no action was taken by the vehicle admin. Applicable to retail experience only.	Show pop-up on key add request expiration NFC key management notifications - no notifications if vehicle is managed by fleet Content of key add request expiration pop-up
Key add - success	Pop-up message informing the user that a key has been added to the vehicle. Applicable to retail experience only.	Content of key add success pop-up NFC key management notifications - no notifications if vehicle is managed by fleet Show pop-up on key add success
Key delete - failed	Pop-up message informing the user that a key deletion request has failed to complete for some reason, even though it was approved by the vehicle admin (or did not require approval in the first place). Applicable to retail experience only.	Show pop-up on key delete failure NFC key management notifications - no notifications if vehicle is managed by fleet Content of key delete failure pop-up Display System: Error screen after user confirms NFC Key Delete request
Key delete - request declined	Pop-up message informing the user that a key deletion request has been denied by the vehicle admin. Applicable to retail experience only.	NFC key management notifications - no notifications if vehicle is managed by fleet Show pop-up on key delete request denial Content of key delete request denial pop-up
Key delete - request expired	Pop-up message informing the user that a key deletion request has expired because no action was taken by the vehicle admin. Applicable to retail experience only.	Show pop-up on key delete request expiration NFC key management notifications - no notifications if vehicle is managed by fleet Content of key delete request expiration pop-up

Key delete - success	Pop-up message informing the user that a key has been deleted from the vehicle. Applicable to retail experience only.	Content of key delete success pop-up Show pop-up on key delete success NFC key management notifications - no notifications if vehicle is managed by fleet
NFC Key Info Screen		Key Info Screen for NFC Device used to start the vehicle NFC key management functions - not available if vehicle is subscribed to fleet NFC management Display System: Conditions to allow "Delete Key" for NFC Info Screen to be enabled NFC Keys Info Screen
Owner Pairing Failed - Pre-Conditions Not Met		Digital Key Owner HMI Event - Pre-Conditions Not Met
Owner Pairing Failed - System Failure		Digital Key Owner HMI Event - System Failure
Owner Pairing Failed - Vehicle Not In Pairing Mode		Digital Key Owner HMI Event - Vehicle Not In Pairing Mode
Owner Pairing Failed - Vehicle Safety Conditions Not Met		Digital Key Owner HMI Event - Vehicle Safety Conditions Not Met
Owner Pairing Finished - Awaiting KTS		Digital Key Owner HMI Event - Awaiting KTS Receipt
Owner Pairing Finished - Key Ready For Use		Digital Key Owner HMI Event - Paired
Owner Pairing Progress		Progress Bar Update
Owner Pairing Starting		Digital Key Owner HMI Event - Start
Personal Profiles Screen	The screens that allow the user to link an NFC device with a vehicle profile. Do behavior: Personal Profiles Linking STM	NFC Card and Personal Profiles NFC Personal Profile Pairing process consistency abort Personal Profile NFC Pairing button Personal Profile NFC Pairing instructions
Prompt to Cancel Key Request		Send HMI Command Request when user confirms request cancellation Confirm request cancellation
Remove NFC Key	The screens that alllow a user to request deletion of an NFC key card or digital key friend device. Do behavior: Remove NFC Key Inner STM	Prompt screen: confirm NFC pairing deletion - actions when confirmed Prompt Screen: No MyKey can pair/change owner device Owner Deletion Warning
Sync Settings Menu	The main settings menu within the In-Vehicle SYNC HMI Screen.	
Unified Key Management Screen	A screen that shows all of the paired NFC access cards and digital keys on the vehicle, as well as keys that have been requested but are not yet approved. Do behavior: Display NFC Key List	List of Keys screen Content for Mobile Device Message Pop-Ups Removing a Mobile Device: analogous to removing NFC Card Mobile Device Message/Pop-up Events Preconditions for Owner Pairing, Changing Owner and Deleting a Mobile Device Prompt Screen: Naming a New NFC Card Owner Deletion Warning Request active and pending NFC Device list NFC key management screen only available while in RUN and motive state

		List of Keys Screen key icons NFC key management functions - not available if vehicle is subscribed to fleet NFC management Unified Key Management Screen - Add/Change Owner Device Factory Key Required To Delete Owner Display System: Conditions to allow "Delete Key" for NFC Info Screen to be enabled Unified Key Management Screen while MyKey in-use Conditions to Enable "Add a Key" Button on Unified Key Management Screen Display "pending" indicator for keys that are pending deletion Unified Key Management Screen for Fleet vehicles
Vehicle Settings Menu	This state describes when the user is in the Vehicle Setting menu within the Setting menu in the In-Vehicle SYNC HMI Screen.	

Table 1: Operation Modes and States on HMI

3.1.2 HMI requirements

REQ-NFC-DK-163 Progress Bar Update

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == ##, the Center Stack Display shall update a progress bar shown on the HMI to notify the user how far in the pairing process they are in.

Acceptance Criteria: Owner Pairing should be inhibited if the vehicle is not ready for pairing

This requirement references the following elements:

- Pairing HMI Event (Enumeration)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-167 Digital Key Owner HMI Event - Start

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Start, the Center Stack Display shall display a message that pairing has started.

This requirement references the following elements:

- Start (Enumeration Literal of Pairing HMI Event)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-168 Digital Key Owner HMI Event - Paired

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Paired, the Center Stack Display shall notify the user that the owner device has been successfully paired and key is ready for use.

This requirement references the following elements:

- Paired (Enumeration Literal of Pairing HMI Event)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-169 Digital Key Owner HMI Event - System Failure

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Failed - System Failure, the Center Stack Display shall notify the user that pairing has failed and should try again.

This requirement references the following elements:

- Failed - System Failure (Enumeration Literal of Pairing HMI Event)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-170 Digital Key Owner HMI Event - Awaiting KTS Receipt

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Awaiting KTS Receipt, the Center Stack Display shall notify the user that the key was created, but not yet active.

This requirement references the following elements:

- Awaiting KTS Receipt (Enumeration Literal of Pairing HMI Event)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-236 Digital Key Owner HMI Event - Vehicle Not In Pairing Mode

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Failed - Vehicle Not In Pairing Mode, the Center Stack Display shall notify the user that pairing has failed due to vehicle not in pairing mode and should try again at the correct vehicle.

Acceptance Criteria: Owner Pairing should be inhibited if the vehicle is not ready for pairing
This requirement references the following elements:

- Owner Pairing Failed - Vehicle Not In Pairing Mode (State)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-237 Digital Key Owner HMI Event - Vehicle Safety Conditions Not Met

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Failed - Vehicle Safety Conditions Not Met, the Center Stack Display shall notify the user that pairing has failed due to vehicle safety conditions not being met and should try again after resolving the issue. The system shall also display the safety requirements.

Acceptance Criteria:
Owner Pairing should not be allowed if vehicle safety conditions have not been established.
This requirement references the following elements:

- Failed - Vehicle Safety Failure (Enumeration Literal of Pairing HMI Event)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-238 Digital Key Owner HMI Event - Pre-Conditions Not Met

If Digital Key Owner Pairing Progress is received by the Center Stack Display with Type == NFC && Result == Failed - Pre-Conditions Not Met, the Center Stack Display shall notify the user that pairing has failed due to pre-conditions not being met and should try again.

Acceptance Criteria: Owner Pairing should be inhibited if a factory key was not used to start the vehicle or if the reader used was not interior.
This requirement references the following elements:

- Owner Pairing Failed - Pre-Conditions Not Met (State)
- Failed - Pre-Conditions Not Met (Enumeration Literal of Pairing HMI Event)
- NFC (Enumeration Literal of Pairing HMI Type)

REQ-NFC-DK-239 Unified Key Management Screen - Add/Change Owner Device

The Unified Key Management screen shall display an option to Add/Change Owner Device based on the following conditions:

- Conditions in REQ-NFC-ES-155 are met, AND
-"Add Owner Device" if there does not exist a Digital Key Record with parameter Key Type == Owner
-"Change Owner Device" if there exists a Digital Key Record with parameter Key Type == Owner

Acceptance Criteria:
the button that dirrects the user to start owner pairing in their device should display:

- Pair Owner Device if no owner device exists on the vehicle
- Change Owner Device if an owner device exists on the vehicle.

This requirement references the following elements:

- Key Type (Property of Digital Key Record)
- Digital Key Type (Enumeration)

REQ-NFC-DK-241 Removing a Mobile Device: analogous to removing NFC Card

Removing a Mobile Device in vehicle shall subscribe to the same behaviors detailed in "Remove NFC Key Inner STM" and subscribe to requirements associated to it.

Acceptance Criteria: Consisten user behavior between NFC Cards and Mobile devices for key termination shall be instituted.

REQ-NFC-DK-242 Content for Mobile Device Message Pop-Ups

The content for the messages described in the following requirements shall substitute "NFC Card" with "Mobile Device" when the device listed has Device Type == Digital Key:

- REQ-NFC-ES-157 Content of key add success pop-up
- REQ-NFC-ES-158 Content of key delete failure pop-up
- REQ-NFC-ES-159 Content of key delete success pop-up
- REQ-NFC-ES-161 Content of key delete request denial pop-up
- REQ-NFC-ES-163 Content of key delete request expiration pop-up
- REQ-NFC-ES-164 Display "pending" indicator for keys that are pending deletion
- REQ-NFC-ES-169 Prompt screen: confirm NFC pairing deletion - actions when confirmed

Acceptance Criteria: Messages that relate to Digital Key Managment should be agnostic or device specific and should not reference Cards for mobile device events.

REQ-NFC-DK-243 Mobile Device Message/Pop-up Events

The Center Stack Display System shall provide the user with a message/pop-up for the following mobile device events:

- REQ-NFC-ES-211 Show pop-up on key add success
- REQ-NFC-ES-212 Show pop-up on key delete failure
- REQ-NFC-ES-213 Show pop-up on key delete success
- REQ-NFC-ES-215 Show pop-up on key delete request denial
- REQ-NFC-ES-217 Show pop-up on key delete request expiration

Acceptance Criteria:
User feed back is required for:

- Mobile Device add events
- Mobile Device delete-failure events
- Mobile Device delete-success events
- Mobile Device delete-denial events
- Mobile Device delete-expiration event

REQ-NFC-DK-244 Preconditions for Owner Pairing, Changing Owner and Deleting a Mobile Device

Mobile Device buttons associated to Pairing an Owner Device, Changing your Owner Device and Deleting the Mobile Device shall subscribe tot he same conditions detailed in REQ-NFC-ES-155

Acceptance Criteria: NFC Key Management screen will only enable the "pair owner device", "change owner device" or "delete mobile device" soft button for Retail vehicles

REQ-NFC-DK-255 Factory Key Required To Delete Owner

If the vehicle is started with Starting Key Type != Factory, the Center Stack Display shall:

- Not allow the user to select "Delete Owner Key"
- Gray out the button to select it
- If the button is selected, provide feedback on what is required to perform this action

This requirement references the following elements:

- Factory Key (Enumeration Literal of NFC Key Type)
- OWNER (Enumeration Literal of Digital Key Type)

REQ-NFC-DK-256 Owner Deletion Warning

If the user selects to delete key with Key Type == Owner and Starting Key Type == Factory, the Center Stack Display shall warn that user that their key will be deleted and they cannot manage friend keys on their mobile device until a new owner device is paired, but they can still be managed on the vehicle with a factory key.

This requirement references the following elements:

- Factory Key (Enumeration Literal of NFC Key Type)
- OWNER (Enumeration Literal of Digital Key Type)

REQ-NFC-ES-4 NFC Keys Info Screen

The NFC Info Screen shall display the following information for each paired NFC device:

- The type of device it is (NFC card or CCC Compliant Device)
- The friendly name of the device
- If the device is an NFC card, the FESN of the card
- If the device is an NFC card, the location of the FESN on the NFC Card
- If the device is an NFC card and a factory card, an indication that it is a factory card
- If the device is a Mobile Device, an indication if it is an Owner or Shared device

Acceptance Criteria: Info pages for device within key management menu has an info button for each key present

REQ-NFC-ES-26 NFC Card and Personal Profiles

An NFC Device shall be associated to “default” profile settings after it is added to the Vehicle.

Acceptance Criteria: Unique Profile not created immediately after NFC Device Add

REQ-NFC-ES-143 NFC key management notifications - no notifications if vehicle is managed by fleet

When the Display System's "NFC Fleet Management Active" configuration parameter is "True", then the Display System shall disable all pop-up notifications related to successfully adding or deleting devices from the vehicle

Acceptance Criteria: HMI does not display a pop-up if Add or Delete operation was completed while NFC Fleet Management is active

REQ-NFC-ES-149 NFC key management functions - not available if vehicle is subscribed to fleet NFC management

When the Display System's "NFC Fleet Management Active" configuration parameter is "True", then the Display System shall disable the "Add NFC Device" and "Delete NFC Device" related soft buttons

Acceptance Criteria: HMI shall disable "Add" and "Delete" soft buttons while NFC Fleet Management is active

REQ-NFC-ES-151 abort Personal Profile NFC Pairing button

The "Personal Profile "Link a Device" screen shall include a cancel/exit/skip button that allows the USER to abort the NFC Personal Profile Pairing process.

Rationale: allow a user to exit the NFC process without setting up a Personal Profile for an NFC device

Acceptance Criteria: Personal profile pairing related screens shall support a cancel button, which can be pressed mid process to exit the profile pairing flow

REQ-NFC-ES-155 Conditions to Enable "Add a Key" Button on Unified Key Management Screen

When the "NFC Enabled on System" configuration parameter of the Display System is "True" and "NFC Fleet Management Active" configuration parameter is "False", the "Unified Key Management" screen shall include the "Add a Key" button.

Rationale: This button allows the user to initiate adding an NFC card to the vehicle.

Acceptance Criteria: NFC Key Management screen will only enable the "Add NFC" soft button for Retail vehicles

REQ-NFC-ES-156 Key add failure pop-up verbiage

The Display System shall have an NFC Feature related center-stack pop-up to indicate a system error at the time of adding an NFC Device, which includes:
- Reason text: "NFC Key Card Add Failed"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification is shown in the error case where the vehicle owner has approved a pairing, but a system error onboard the vehicle prevented the pairing from being completed. The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that is the subject of the notification.

Acceptance Criteria: Key add fail pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-157 Content of key add success pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate successful adding an NFC Device, which includes:
- Reason text: "NFC Key Card Add Successful"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification lets the user know that the card is ready for use in the vehicle. The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that has been added.

Acceptance Criteria: Key add successful pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-158 Content of key delete failure pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate a system error at the time of deleting an NFC Device, which includes:
- Reason text: "NFC Key Card Delete Failed"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification is shown in the error case where the vehicle owner has approved an unpairing, but a system error onboard the vehicle prevented the unpairing from being completed. The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that has been added

Acceptance Criteria: A system failure resulting in an NFC Key not being able to be deleted from the vehicle will result in an in-vehilce pop-up indicating that an error occurred

REQ-NFC-ES-159 Content of key delete success pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate successful deletion of an NFC Device, which includes:
- Reason text: "NFC Key Card Delete Successful"
- The FESN or Friendly name of the selected NFC Key Card

Acceptance Criteria: Key delete successful pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-160 Content of key add request denial pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate the admin has denied the NFC Key Add request which includes:
- Reason text: "NFC Key Card Add Request Denied"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification is shown in the case where the vehicle owner has explicitly denied a request to add a key. The card is not usable to enter and start the vehicle.

The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that is the subject of the notification.

Acceptance Criteria: Key add denial pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-161 Content of key delete request denial pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate the admin has denied the NFC Key Delete request which includes:
- Reason text: "NFC Key Card Delete Request Denied"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification is shown in the case where the vehicle owner has explicitly denied a request to unpair a key. The card is still usable to enter and start the vehicle.

The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that is the subject of the notification.

Acceptance Criteria: Key delete denial pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-162 Content of key add request expiration pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate the admin did not respond to the NFC Key Add request within a specific time frame, which includes:
- Reason text: "NFC Key Card Add Request Timed Out"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification is shown in the error case where the vehicle owner has not approved a request to unpair a key and the request has expired. The card is still usable to enter and start the vehicle.

The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that is the subject of the notification.

Acceptance Criteria: Key add expiration pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-163 Content of key delete request expiration pop-up

The Display System shall have an NFC Feature related center-stack pop-up to indicate the admin did not respond to the NFC Key Delete request within a specific time frame, which includes:
- Reason text: "NFC Key Card Delete Request Timed Out"
- The FESN or Friendly name of the selected NFC Key Card

Rationale: This notification is shown in the error case where the vehicle owner has not approved a request to unpair a key and the request has expired. The card is still usable to enter and start the vehicle.

The FESN should be included because multiple card requests can be pending simultaneously - the FESN uniquely identifies the card that is the subject of the notification.

Acceptance Criteria: Key delete expiration pop-up will be dismissable and indicate for which device it was for.

REQ-NFC-ES-164 Display "pending" indicator for keys that are pending deletion

Key pairings which have an outstanding deletion request shall appear in the Unified Key Management Screen with an icon or other status indicator to show that they are pending deletion.

Acceptance Criteria: Card pairing which has an outstanding deletion request appears with icon or annotation

REQ-NFC-ES-168 Display System: Error screen after user confirms NFC Key Delete request

If either of the following occurs:
- The user presses the "delete key" button for a paired NFC device while the vehicle does not have network connectivity
- While the Display System is displaying the "Wait for NFC Controller" screen in the NFC card delete flow, it receives a Pairing Status message with the "Controller Status" value set to "Fault - No Connectivity"

then the Display System shall display a message indicating that there is no network connectivity, and NFC keys can only be deleted from the vehicle when there is network connectivity. Dismissing this message shall return to the Unified Key Management Screen or the key information screen where the user pressed the delete button.

Rationale: Informs user that request to delete key has failed due to lack of network connectivity or because of a system timeout

Acceptance Criteria: In-vehicle HMI shall not initiate NFC Device Delete request if there is no vehicle connectivity at the time of request

REQ-NFC-ES-169 Prompt screen: confirm NFC pairing deletion - actions when confirmed

If the Display System is displaying the Remove NFC Key - Confirm Delete screen in the NFC card delete flow, and the user presses the Confirm button (or equivalent), the Display System shall:
- Transmit an HMI Command Request message with:
  - the FESN value set or key ID to the Pairing ID of the pairing the user has selected for deletion
  - the Friendly Name value empty/null
  - the Command Type value set to "Delete Pairing"
- Transition to the "Wait for NFC Controller" screen

Rationale: Informs user that request to delete key has been processed

REQ-NFC-ES-171 Display System: Conditions to allow "Delete Key" for NFC Info Screen to be enabled

The NFC Key Info screen shall include a control that allows the user to request deletion of the key being displayed.

The delete control shall only appear when:
The key is not a factory key to the vehicle
The key record represents an active pairing (not pending add or pending delete)

The delete control shall only be enabled when all of the following are true:

- Vehicle is in RUN ignition state
- Vehicle modem is authorized
- Vehicle has network connectivity
- The key that was used to start the vehicle is not a MyKey
- "NFC fleet management active" configuration parameter of the Display System is False
- "NFC Key Type" of the key selected for deletion is not "Factory Key"
- The key selected for deletion was not used to start the vehicle (in the current drive cycle)
- (FIXME: The starting key is not a friend key)

Acceptance Criteria: "Delete" Key shall be displayed under NFC Key info menu, while vehicle is in run, for each key that is not a factory keys, and not a fleet user key

REQ-NFC-ES-172 Enable NFC MyKey Softbuttons

The Display system shall update its "Create MyKey" page to "grey out" the "Create NFC MyKey" related soft buttons while the following conditions are true:
- Current MyKey Level == MyKey

Rationale: NFC related MyKey softbuttons should only be available for Retail Vehicles with the NFC Feature

Acceptance Criteria: "Create MyKey" button is greyed out after vehicle started with MyKey

REQ-NFC-ES-183 List of Keys screen

The list of keys screen shall display one list entry for each vehicle key, including key fobs, PaaK Keys, NFC Devices.

REQ-NFC-ES-184 List of Keys Screen key icons

Each list item in List of Keys Screen shall have an icon representing the type of item. (i.e. key fob, NFC User Card, NFC Factory Card, Phone)

REQ-NFC-ES-197 NFC Personal Profile Pairing process consistency

The Display System shall ensure the NFC Personal Profile Pairing process is consistent with current Personal Profile Device Pairing

Rationale: NFC is a tie-in to already existing Personal Profile process. The Display system shall incorporate NFC as an alternative device maintain consistency.

REQ-NFC-ES-198 Personal Profile NFC Pairing instructions

The "Personal Profile "Link a Device" screen shall include instructions to pair an NFC device. The instructions shall include at minimum:

- Tap NFC device in interior reader
note: exact wording shall be reviewed by and concurred with HMI.

Rationale: provide instructions on how to pair an NFC device to the users personal profiles

Acceptance Criteria: In-vehicle HMI shall prompt the user to scan the interior reader as part of pairing a profile to the NFC Device

REQ-NFC-ES-204 Prompt Screen: Naming a New NFC Card

When a user presses the "Add a Key" button on the Unified Key Management Screen, and all of the following are true:

- The vehicle has network connectivity
- The vehicle's ignition is in RUN
- The key that started the vehicle is not a MyKey
- The "NFC Fleet Management Active" configuration parameter of the Center Stack Display System is False

then the Display System shall show the "Add a Key - enter friendly name" screen.

Rationale: This screen prompts the user to name the new NFC card during the key add flow.

Acceptance Criteria: Pressing "Add a Key" Button results in HMI showing keyboard appropriate to local language and accepts user input for NFC Device "Friendly Name"

REQ-NFC-ES-210 Show pop-up on key add failure

When the Display System receives an NFC Local Event message and all of the following are true:

- The "Successful" signal of the NFC Local Event message is False
- The "Command Type" signal of the NFC Local Event message is "Add Key"
- The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC card pairing failed to complete.

Rationale: This notification is shown in the error case where the vehicle owner has approved a pairing, but a system error onboard the vehicle prevented the pairing from being completed. The card may not be usable to enter and start the vehicle.

Acceptance Criteria: A system failure resulting in an NFC Key not being able to be added to the vehicle will result in an in-vehicle pop-up indicating that an error occurred

REQ-NFC-ES-211 Show pop-up on key add success

When the Display System receives an NFC Local Event message and all of the following are true:

- - The "Successful" signal of the NFC Local Event message is True
- - The "Command Type" signal of the NFC Local Event message is "Add Key"
- - The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC card pairing was successful.

Acceptance Criteria: A request being approved and successfully completed resulting in an NFC Key being added to the vehicle will result in an vehicle pop-up indicating that the request was successfully completed
This requirement references the following elements:

- NFC Local Event (Logical Signal)

REQ-NFC-ES-212 Show pop-up on key delete failure

When the Display System receives an NFC Local Event message and all of the following are true:

- The "Successful" signal of the NFC Local Event message is False

- The "Command Type" signal of the NFC Local Event message is "Delete Key"
- The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC card unpairing failed to complete.

Rationale: This notification is shown in the error case where the vehicle owner has approved an unpairing, but a system error onboard the vehicle prevented the unpairing from being completed. The card may still be usable to enter and start the vehicle.

Acceptance Criteria: A system failure resulting in an NFC Key not being able to be deleted from the vehicle will result in an in-vehicle pop-up indicating that an error occurred
This requirement references the following elements:

- NFC Local Event (Logical Signal)
- NFC fleet management active (Runtime Variable)

REQ-NFC-ES-213 Show pop-up on key delete success

When the Display System receives an NFC Local Event message and all of the following are true:

- The "Successful" signal of the NFC Local Event message is True
- The "Command Type" signal of the NFC Local Event message is "Delete Key"
- The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC key unpairing was successful.

Acceptance Criteria: A request being approved and successfully completed resulting in an NFC Key being deleted from the vehicle will result in an in-vehicle pop-up indicating that the request was successfully completed
This requirement references the following elements:

- NFC Local Event (Logical Signal)
- NFC fleet management active (Runtime Variable)

REQ-NFC-ES-214 Show pop-up on key add request denial

When the Display System receives an Retail User Approval Status message and all of the following are true:

- - The "Request Status" signal of the Retail User Approval Status message is "Denied"
- - The "Request Type" signal of the Retail User Approval Status message is "Add Key"
- - The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC card pairing was not approved because the retail owner did not reply to the request.

Rationale: This notification is shown in the case where the vehicle owner has explicitly denied a request to pair a key. The card is not usable to enter and start the vehicle.

Acceptance Criteria: An admin rejection resulting in an NFC Key not being able to be added to the vehicle will result in an in-vehicle pop-up indicating that the request was rejected

REQ-NFC-ES-215 Show pop-up on key delete request denial

When the Display System receives an Retail User Approval Status message and all of the following are true:

- The "Request Status" signal of the Retail User Approval Status message is "Denied"
- The "Request Type" signal of the Retail User Approval Status message is "Delete Key"
- The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC key unpairing was not approved because the retail owner explicitly denied the request.

Rationale: This notification is shown in the case where the vehicle owner has explicitly denied a request to unpair a key. The card is not usable to enter and start the vehicle.

Acceptance Criteria: An admin rejection resulting in an NFC Key not being able to be deleted from the vehicle will result in an in-vehicle pop-up indicating that the request was rejected

REQ-NFC-ES-216 Show pop-up on key add request expiration

When the Display System receives an Retail User Approval Status message and all of the following are true:

- The "Request Status" signal of the Retail User Approval Status message is "Timed out"
- - The "Request Type" signal of the Retail User Approval Status message is "Add Key"
- - The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC card pairing was not approved because the retail owner did not reply to the request.

Rationale: This notification is shown in the error case where the vehicle owner has not approved a request to pair a key and the request has expired. The key is not usable to enter and start the vehicle.

Acceptance Criteria: A request timeout resulting in an NFC Key not being able to be added to the vehicle will result in an in-vehicle pop-up indicating that the request has timed out

REQ-NFC-ES-217 Show pop-up on key delete request expiration

When the Display System receives an Retail User Approval Status message and all of the following are true:

- The "Request Status" signal of the Retail User Approval Status message is "Timed out"
- The "Request Type" signal of the Retail User Approval Status message is "Delete Key"
- The "NFC Fleet Management Active" configuration parameter of the Display System is False

then the Display System shall show a pop-up indicating that the user's requested NFC key unpairing was not approved because the retail owner did not reply to the request.

Rationale: This notification is shown in the error case where the vehicle owner has not approved a request to unpair a key and the request has expired. The card is still usable to enter and start the vehicle.

Acceptance Criteria: A request timeout resulting in an NFC Key not being able to be deleted from the vehicle will result in an in-vehicle pop-up indicating that the request has timed out

REQ-NFC-ES-236 Unified Key Management Screen for Fleet vehicles

The Display system shall update its Unified Key Management Screen to only display a list of (NFC) keys programmed to the vehicle and hide all the "Add NFC Device" related soft buttons while the following conditions are true:
- Display System configuration parameter "NFC Fleet Management active" == True

Rationale: Fleet vehicles cannot (aren't allowed) to use the in-vehicle HMI to add or delete NFC devices.

REQ-NFC-ES-237 Unified Key Management Screen while MyKey in-use

The Display system shall update its Unified Key Management Screen to "grey out" the "Add NFC Device" related soft buttons while the following conditions are true:
- Current MyKey Level == MyKey

Rationale: MyKey user is not allowed to Add or Remove NFC Devices from the vehicle

REQ-NFC-ES-240 Key Info Screen for NFC Device used to start the vehicle

The Display system shall update its "Key Info Screen" to "grey out" the "Delete NFC Device" related soft buttons, for the NFC Key used to start the vehicle. while the following conditions are true:
- Ignition status == Run

Rationale: User cannot delete the NFC key they used to start the vehicle

REQ-NFC-ES-302 Request active and pending NFC Device list

When the user selects to enter the Unified Key Management Screen within the HMI, the Display System shall transmit a "Request NFC Devices List" message to the NFC system requesting for a list of the Active and Pending NFC Devices on the vehicle.

Acceptance Criteria: In-vehicle HMI shall have a key management screen for NFC Keys under vehicle settings menu

REQ-NFC-ES-337 NFC key management screen only available while in RUN and motive state

The NFC key management screen and its functions shall only be accessible when the ignition state is RUN and motive state..

Acceptance Criteria: NFC Key Management menu is under "Vehicle Settings" menu and accessible only in RUN

REQ-NFC-ES-434 Prompt Screen: Change Owner Device

When user selects "Change Owner Device", the Display System shall provide instructions on how to change an owner device and provide a way for the user to initiate the process, such as a QR code.

REQ-NFC-ES-435 Prompt Screen: No MyKey can pair/change owner device

The Display System shall disable the "Change Owner Device"/"Add Owner Device" AND "Add Key" button when a MyKey user is active.

REQ-NFC-ES-444 Prompt Screen: Add Owner Device

When user selects "Add Owner Device", the Display System shall provide instructions on how to pair an owner device and provide a way for the user to initiate the process, such as a QR code.

REQ-NFC-ES-449 Send HMI Command Request when user confirms request cancellation

If the user activates the "cancel request" control defined in REQ-NFC-ES-450 and confirms their intent to cancel (by approving the resulting dialog box or equivalent), the Center Stack Display System shall transmit an HMI Command Request message to the NFC Controller, with the following parameters:

- Friendly Name: null
- Requested Command Type: Cancel Request
- Pairing ID: null
- Local ID: the Local ID associated with the request that the user is canceling

This requirement references the following elements:

- HMI Command Request (Logical Signal)
- Confirm request cancellation (System Requirement)
- Pairing ID (Property of HMI Command Request)
- Local ID (Property of HMI Command Request)
- Cancel Request (Enumeration Literal of NFC Command Type)
- Requested Command Type (Property of HMI Command Request)
- Friendly Name (Property of HMI Command Request)

REQ-NFC-ES-450 Confirm request cancellation

When a user activates the cancel control on a list entry whose status is "pending add" or "pending delete", the Center Stack Display shall prompt the user to confirm the request before transmitting a cancellation as described in REQ-NFC-ES-449.

This requirement references the following elements:

- NFC Devices List (Logical Signal)
- Send HMI Command Request when user confirms request cancellation (System Requirement)

3.2 Logical System Properties

3.2.1.1 Configuration Parameters

Parameter name	Data type	Description
MyKey Creation Body Control System Response Timeout	period duration	When the user triggers the MyKey creation flow, and after the Display System sends the message initiating the MyKey creation process on the BCM, the duration that the Display System will wait for a response from the BCM before aborting and displaying an error.
NFC Card Add NFC Controller Response Timeout	period duration	The maximum duration that the Center Stack Display System will wait for a response from the NFC Controller after it sends an HMI Command Request. If no response is received, the Center Stack Display System will display an error.

3.2.1.2 Runtime Variables

Variable name	Data type	Description
NFC fleet management active	Boolean	Active = Vehicle is enrolled in "NFC Fleet Management" subscription Inactive = Vehicle is not enrolled in "NFC Fleet Management" subscription
Ignition On	Boolean	Whether or not the in-vehicle center stack display is powered on and ready to display content to the user.
MyKey State	MyKey Level	
Starting Key Type	NFC Key Type	
Ignition Status	Ignition Status	
Gear Shift Position		
Modem Authorized	Boolean	
NFC Feature Enabled	Boolean	

3.3 Logical System Requirements

REQ-NFC-ES-4 NFC Keys Info Screen

The NFC Info Screen shall display the following information for each paired NFC device:

- The type of device it is (NFC card or CCC Compliant Device)
- The friendly name of the device
- If the device is an NFC card, the FESN of the card
- If the device is an NFC card, the location of the FESN on the NFC Card
- If the device is an NFC card and a factory card, an indication that it is a factory card
- If the device is a Mobile Device, an indication if it is an Owner or Shared device

Acceptance Criteria: Info pages for device within key management menu has an info button for each key present

REQ-NFC-ES-24 A MyKey cannot create a MyKey

If the Vehicle was started with a MyKey, functions for creating another MyKey shall be disabled.

Acceptance Criteria: "Create MyKey" softbuttons not present while MyKey in use

REQ-NFC-ES-35 Modal return to previous screen

When a modal is dismissed or timed-out, the In-Vehicle HMI System shall return to the previous screen.

Acceptance Criteria: Dismissing a NFC related pop-up will return HMI to previous screen/menu

REQ-NFC-ES-44 Do not wake HMI when vehicle is off

The NFC Command Complete Event shall not wake the HMI System if the vehicle is off.

Acceptance Criteria: Centerstack display remains OFF while ignition is off and NFC Command Complete Event is true

REQ-NFC-ES-50 Master Reset - User Initiation Limitation

If the vehicle was started with any of the following key types:
- MyKey
- User Key

then functions for Master Reset shall be disabled.

Acceptance Criteria: Master Reset softbutton greyed out while MyKey in use

REQ-NFC-ES-83 Retail users not allowed to remove Factory Keys

The Center Stack Display shall check whether the NFC Key to be deleted in a Retail Request is a Factory Key and shall reject the request if so.

Acceptance Criteria: NFC Key Management menu does not display "Delete" button within factory key info drop down

REQ-NFC-ES-92 MyKey Users not allowed to add or remove NFC Key

If the Vehicle was started using a MyKey, the Remove NFC Key Screen and the Add NFC Card Screen shall be inaccessible until the Vehicle is started with a Standard Key.

Acceptance Criteria: NFC Key Management screen "Add" and "Delete" softbuttons for each indvidual key are greyed out while MyKey is in use

REQ-NFC-ES-129 NFC key management functions only available if modem is authorized

The Key Management screen "Add an NFC Key" or "Delete an NFC Key" soft-buttons/functions shall only be available while the modem is authorized and the vehicle is not enrolled into the "NFC Fleet Management" feature

Acceptance Criteria: NFC Key Management Menu displays Add and Delete related soft buttons while modem authorized and not enrolled in fleet. If modem not authorized OR enrolled in fleet, buttons are disabled

REQ-NFC-ES-179 Feature availability for Personal Profile linking

When "NFC Enabled on System" configuration parameter of the Display System == True, the Display System shall provide NFC related Enhanced Memory screens according to section 4.5.2.3 of the Enhanced Memory APIM SPSS

Rationale: ensure NFC features are available on the vehicle before allowing a NFC device to be setup as a Personal Profile

Acceptance Criteria: Vehicles equipped with the NFC Feature shall support pairing NFC Devivces to their profiles

REQ-NFC-ES-189 NFC Feature specific pop-up classifications and duration

All NFC Feature related center-stack pop-ups are:

- Non-critical
- Non-safety related
- User dismiss-able
- Timed for 5 seconds

The HMI team will determine the specific "Reason Text" for each of these pop-ups
Any exceptions to these will be called out within separate requirements for the specific pop-up

Acceptance Criteria: All NFC Feature related center-stack pop-ups are: - Non-critical - Non-safety related - User dismiss-able - Timed for 5 seconds

REQ-NFC-ES-307 Locking and starting function even without display system

The NFC system shall fulfill the unlocking, locking, and vehicle starting functions without depending on communications with, or the operation of, the in-vehicle display system.

Acceptance Criteria: Enter and Start the vehicle with missing or disconnected Sync module

REQ-NFC-ES-337 NFC key management screen only available while in RUN and motive state

The NFC key management screen and its functions shall only be accessible when the ignition state is RUN and motive state..

Acceptance Criteria: NFC Key Management menu is under "Vehicle Settings" menu and accessible only in RUN

REQ-NFC-ES-435 Prompt Screen: No MyKey can pair/change owner device

The Display System shall disable the "Change Owner Device"/"Add Owner Device" AND "Add Key" button when a MyKey user is active.

REQ-NFC-ES-458 Display Deletion Notification To User If Starting Key

If the Center Stack Display receives a NFC Local Event with:

- Command Type == Delete Key
- Outcome == True - Starting Key

then the Center Stack Display shall notify the user that the key used to start the vehicle was deleted.

Acceptance Criteria: HMI popup displays message stating that the device used to start the vehicle has been deleted.

4 FUNCTION SPECIFICATIONS

Function Name	Function Description
Add NFC key InnerSTM <<>>	
HMI <<>>	The screens and flows of the in-vehicle display system that are relevant to the NFC Entry and Starting feature.
MyKey Management Inner STM <<>>	
Personal Profiles Linking STM <<>>	
Remove NFC Key Inner STM <<>>	

4.1 Add NFC key InnerSTM

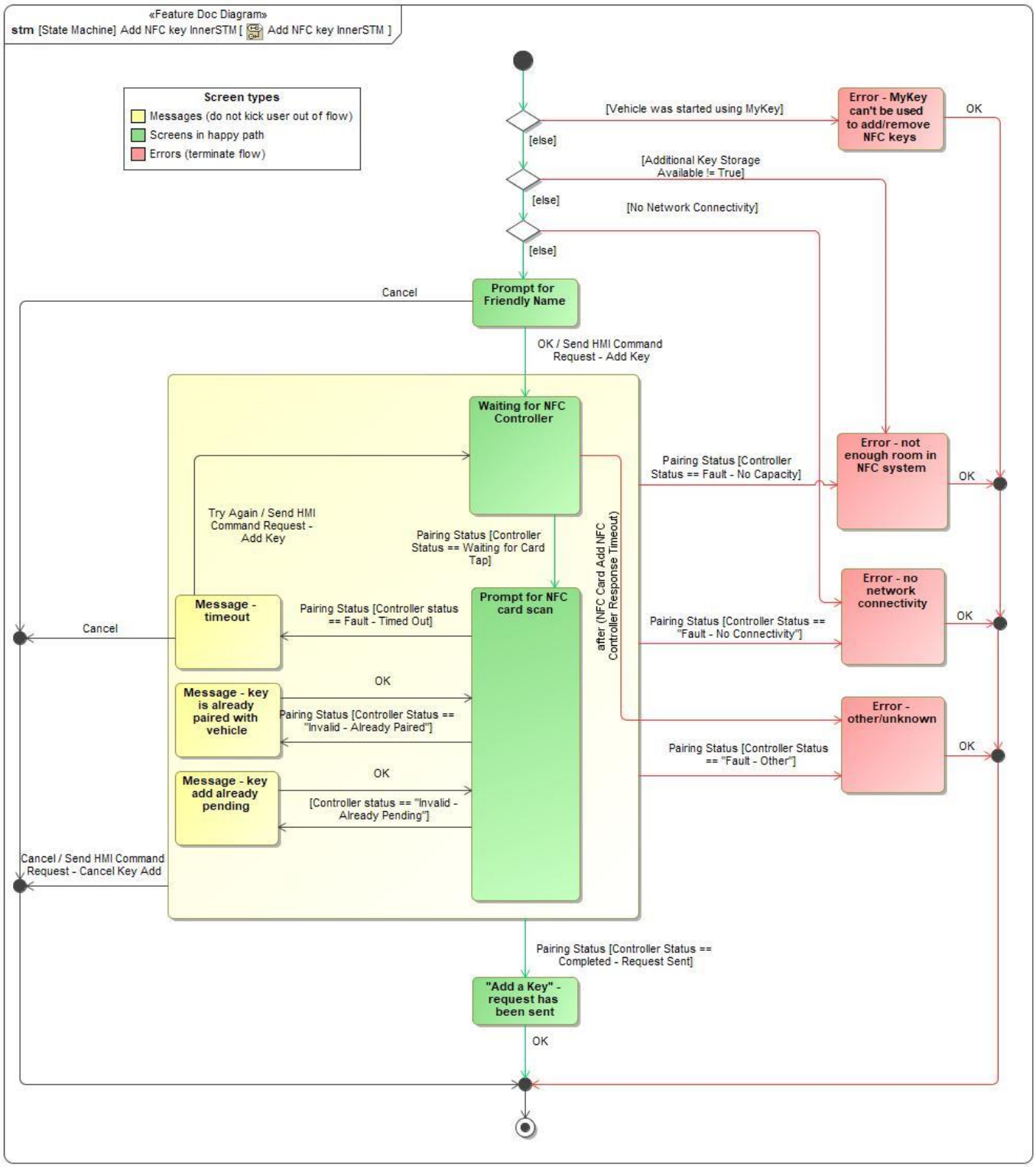


Figure 4: Add NFC key InnerSTM

4.1.1 Add NFC key InnerSTM Screens

State	Description	Requirements Reference
"Add a Key" - request has been sent		Progress Screen: Add Request Sent Progress Screen: Waiting for Controller Ready
Error - MyKey can't be used to add/remove NFC keys		Error Screen: Attempting to add or delete a key when MyKey restrictions are active
Error - no network connectivity		Error Screen: Attempting to Add or Delete Keys When There Is No Network Connectivity
Error - not enough room in NFC system		Error Screen: Selecting "Add a Key" Button When Key Storage is Full
Error - other/unknown		Error Screen: Other Error during NFC Card Add
Message - key add already pending		Error Screen: NFC Card Already Has Pending Request
Message - key is already paired with vehicle		Error Screen: Scanning an Existing NFC Card
Message - timeout		Error Screen: Timeout Waiting for NFC Card Scan - Actions Error Screen: Timeout Waiting for NFC Card Scan
Prompt for Friendly Name		Friendly name input - strip leading and trailing whitespace Friendly Name input - placeholder/default input Character encoding Prompt Screen: Naming a New NFC Card Sending Request screen - transmit HMI Command Request signal Friendly name input - requirements
Prompt for NFC card scan		Prompt Screen: Prompt for NFC Card Scan - actions Error Screen: NFC Card Already Has Pending Request Progress Screen: Add Request Sent Progress Screen: Waiting for Controller Ready Prompt Screen: Prompt for NFC Card Scan
Waiting for NFC Controller		Prompt Screen: Prompt for NFC Card Scan - actions Sending Request screen - transmit HMI Command Request signal

Table 2: Operation Modes and States on Add NFC key InnerSTM

4.1.2 Add NFC key InnerSTM requirements

REQ-NFC-ES-154 Character encoding

The input field for NFC Card friendly name shall support up to 64 UTF-8 characters.

REQ-NFC-ES-174 Error Screen: Scanning an Existing NFC Card

If the Display System is displaying the "Prompt for NFC Card Scan" screen and it receives a Pairing Status message with the "Controller Status" value set to "Invalid - Already Paired", then the Display System shall show a message indicating that the card scanned by the user is already paired with the vehicle, and cannot be re-added.

Dismissing this message shall cause the Display System to return to the "Prompt for NFC Card Scan" screen.

Rationale: This screen informs the user that the scanned NFC card is already paired to the vehicle.

Acceptance Criteria: Scanning an already-paired NFC card while the display is prompting for a card scan causes a dismissable message to show, with text indicating that the card is already paired

REQ-NFC-ES-175 Error Screen: Attempting to add or delete a key when MyKey restrictions are active

When the key that started the vehicle is a MyKey, and either of the following occurs:

A user presses the disabled "Add NFC Card" button on the Unified Key Management Screen
A user presses the disabled "Remove NFC Key" button (or equivalent) on the Unified Key Management Screen or a key info screen

the Display System shall display a message indicating that NFC pairings and unpairings are not allowed while MyKey restrictions are active.

The message should inform the user that they need to shut off the vehicle and start it with a key that is not a MyKey in order to manage NFC pairings.

Dismissing the message shall return the Display System to the Unified Key Management Screen.

Rationale: This screen informs the user that NFC cards cannot be added to the vehicle when MyKey is active.

Acceptance Criteria: In-vehicle HMI will grey out "Add a Key" and key delete buttons when MyKey is in use; pressing the disabled buttons causes a message to display

REQ-NFC-ES-176 Error Screen: Selecting "Add a Key" Button When Key Storage is Full

When either of the following occurs:

- The user presses the "Add NFC Card" button in the Unified Key Management Screen, but the "Additional Key Storage Available" value of the most recently received "NFC Devices List" message is False
- While the Display System is displaying the "Waiting for NFC Controller" or "Prompt for NFC card scan" screens, it receives a "Pairing Status" message with the "Controller status" value set to "Fault - No Capacity"

then the Display System shall display a message to the user indicating that the maximum number of NFC pairings has been reached, and they need to delete some existing pairings if they wish to create another.

Dismissing this message shall return the user to the Unified Key Management Screen.

Rationale: This screen informs the user that key storage is full when they attempt to add an NFC card.

Acceptance Criteria: Pressing Add a Key button within in-vehicle HMI shall not start the key pairing process and display a pop-up indicating not enough room in NFC system (when no key storage is available on NFC system)

REQ-NFC-ES-178 Error Screen: Attempting to Add or Delete Keys When There Is No Network Connectivity

When any of the following occurs:

- The user presses the "Add NFC Card" button on the Unified Key Management Screen and the vehicle has no network connectivity

- The user presses the "Delete NFC Key" button (or equivalent) on the Unified Key Management Screen or a NFC key info screen
- While the HMI is displaying the "Waiting for NFC Controller" screen in the NFC key add or NFC key delete flows, or the "Prompt for NFC card scan" screen in the NFC key add flow, it receives a Pairing Status message with the "Controller Status" value == "Fault - No Connectivity"

then the Display System shall display a message to the user indicating that there is no network connectivity, and NFC cards cannot be added or deleted when there is no network connectivity.

Dismissing this message shall return a user to the Unified Key Management Screen.

Rationale: User guidance when key adds are not allowed

Acceptance Criteria: Pressing "Add a Key" button or any NFC key delete button within in-vehicle HMI shall not start the key pairing process and display a pop-up indicating vehicle has no connectivity

REQ-NFC-ES-204 Prompt Screen: Naming a New NFC Card

When a user presses the "Add a Key" button on the Unified Key Management Screen, and all of the following are true:

- The vehicle has network connectivity
- The vehicle's ignition is in RUN
- The key that started the vehicle is not a MyKey
- The "NFC Fleet Management Active" configuration parameter of the Center Stack Display System is False

then the Display System shall show the "Add a Key - enter friendly name" screen.

Rationale: This screen prompts the user to name the new NFC card during the key add flow.

Acceptance Criteria: Pressing "Add a Key" Button results in HMI showing keyboard appropriate to local language and accepts user input for NFC Device "Friendly Name"

REQ-NFC-ES-205 Progress Screen: Waiting for Controller Ready

When the HMI is displaying the "Add a Key - enter friendly name" screen and the user presses the "Next" button after entering a valid friendly name, the Display System shall:

- Send an "HMI Command Request" message with "Friendly Name" set to the user-entered friendly name, "Requested Command Type" set to "Add Key", and "FESN" null
- Display the "Waiting for NFC Controller" screen

Rationale: This screen informs the user of the progress of the key add request.

Acceptance Criteria:
Pressing "Next" button (or equivalent) results in HMI transmitting message to NFAM and switching to "Waiting for NFCController"screen

REQ-NFC-ES-206 Prompt Screen: Prompt for NFC Card Scan

When the Display System is displaying the "Waiting for NFC Controller" screen, and the Display System receives a "Pairing Status" message with the "Controller Status" value set to "Waiting for Card Tap", the Display System shall display the "Add a Key" screen - prompt for NFC card" screen.

Rationale: This screen prompts the user to scan a new NFC card during the key add flow.

Acceptance Criteria: Display transitions from "Waiting"/"Loading" to "Scan NFC Card" when "Card Pairing Status" message is received with "Controller Status"== "Waiting for Card Tap"

REQ-NFC-ES-218 Progress Screen: Add Request Sent

When the Display System is displaying the "Prompt for NFC Card Scan" screen of the NFC card add flow, and it receives a "Pairing Status" message with the "Controller Status" value set to "Completed - Request Sent", it shall display a message to the user indicating that:

- The card add request has been sent successfully
- The card cannot be used until the vehicle owner approves the request on their mobile device

Acceptance Criteria: Display changes from card scan prompt to success message when Card Pairing Status message is received as described in requirement

REQ-NFC-ES-226 Sending Request screen - transmit HMI Command Request signal

When the Center Stack Display System transitions to displaying the "Sending Request" screen during the flow to add a new NFC key card, the Center Stack Display System shall immediately transmit an "HMI Command Request" message with the following signals:

- Friendly Name = The friendly name that the user has status for the new key in the preceding screens
- FESN = The "FESN" signal value of the "NFC Tap" message that triggered the transition into this state
- Command Type: Add Key

Rationale: This message hands off the add-key flow to the NFC System, which handles request transmission after this point

REQ-NFC-ES-346 Error Screen: NFC Card Already Has Pending Request

When the Display System is displaying the "Prompt for NFC Card Scan" screen in the NFC card add flow, and it receives a "Pairing Status" message with the "Controller Status" value set to "Invalid - Already Pending", it shall display a message to the user indicating that they cannot add the card that was just tapped because it already has an outstanding add request.

Dismissing this message shall return the Display System to the "Prompt for NFC Card Scan" screen.

Acceptance Criteria: Attempting to create an add request for the same card twice in a row causes this message to appear

REQ-NFC-ES-347 Error Screen: Other Error during NFC Card Add

When any of the following occurs:

- While the Display System is displaying the "Waiting for NFC Controller" or "Prompt for NFC Card Scan" screens, it receives a "Pairing Status" message with the "Controller Status" value set to "Fault - Other"
- More time than the duration specified in the "NFC Card Add NFC Controller Response Timeout" parameter passes after the Display System sends the "HMI Command Request" message during the NFC card add flow

then the Display System shall display a message to the user indicating that an unknown error has occurred during the NFC card add process and they cannot continue.

Dismissing this message shall return the Display System to the Unified Key Management Screen.

Acceptance Criteria: Attempting to add NFC card while NFC Controller is disconnected causes error message to display after timeout duration

REQ-NFC-ES-348 Prompt Screen: Prompt for NFC Card Scan - actions

The "Prompt for NFC card scan" and "Waiting for NFC Controller" screens in the NFC card add flow shall have a button or action labeled "Cancel" (or equivalent).

Pressing this button shall:

- Transmit an "HMI Command Request" message with the Friendly Name value set to null, the FESN value set to null, and the Command Type value set to "Cancel Key Add"
- Return the user to the Unified Key Management Screen

Acceptance Criteria: Users are able to escape from NFC card add flow after typing in friendly name without needing to wait for the entire timeout duration. NFC Controller receives cancellation request when cancel button is pressed.

REQ-NFC-ES-349 Error Screen: Timeout Waiting for NFC Card Scan

If the Display System is displaying the "Prompt for NFC Card Scan" screen in the NFC card add flow, and it receives a "Pairing Status" message with the "Controller Status" value set to "Fault - Timed Out", then it shall display the "Message - timeout" screen.

Acceptance Criteria: Waiting for longer than NFC controller timeout at the NFC card scan screen results in this message being shown

REQ-NFC-ES-350 Error Screen: Timeout Waiting for NFC Card Scan - Actions

The "Message - timeout" screen/warning in the NFC card add flow shall have at least the following buttons/actions:

- "Cancel Add" or equivalent text. Pressing this button shall return the user to the Unified Key Management screen.
- "Try Again" or equivalent text. Pressing this button shall cause the Display System to:
  - Transmit an "HMI Command Request" message with the Friendly Name entered by the user earlier in the flow, no FESN, and the Command Type value set to "Add Card"
  - Transition to the "Waiting for NFC Controller" screen

Acceptance Criteria: After timeout occurs waiting for card scan, user is able to restart key add flow by pressing "Try Again" button

REQ-NFC-ES-431 Friendly name input - requirements

The user input controls on the friendly name input screen shall enforce the following requirements:

- The friendly name shall not be zero length.
- The friendly name shall not consist only of whitespace characters.
- The friendly name shall not consist of any more than 64 characters after any leading and trailing whitespace have been removed from the input.
- The friendly name shall not be identical to any of the other friendly names in the most recently received list of keys (including pending/requested keys), after any leading and trailing whitespace have been removed from the input.

If all of these requirements are not satisfied by the user's friendly name input, the HMI shall not allow the user to proceed beyond the friendly name input screen.

This requirement references the following elements:

- NFC Devices List (Logical Signal)
- Friendly Name (Value Property)
- Friendly Name (Runtime Variable)

REQ-NFC-ES-432 Friendly name input - strip leading and trailing whitespace

When the user provides a friendly name input on the Prompt for Friendly Name screen, the HMI shall remove leading and trailing whitespace characters from the user input before transmitting it or storing it.

REQ-NFC-ES-433 Friendly Name input - placeholder/default input

When a user enters the Prompt for Friendly Name screen during the card add flow, the input control shall be pre-populated with a default name as follows:

If the most recent list of keys received from the NFC module has no pairing records or pending pairing records whose Friendly Name is exactly "Key Card #", where "#" is any integer, the default name shown shall be "Key Card 1".

Otherwise, the default name shown shall be "Key Card *n*", where *n* is the largest "Key Card #" number present in the list of pairing records and pending pairing records, plus one.

For example: If the most recently received key list contains the following entries:

Entry Type	Friendly Name
Pairing	Factory Card 1
Pairing	Factory Card 2
Pairing	Aaron's Favorite Key
Pairing	Key Card 1
Pairing	Key Card 2
Pending deletion	Key Card 2
Pending addition	Key Card 3

then the pre-populated name on the Prompt for Friendly Name screen shall be "Key Card 4".

This requirement references the following elements:

- NFC Devices List (Logical Signal)
- Friendly Name (Value Property)
- Friendly Name (Runtime Variable)
- Active NFC Devices (Property of NFC Devices List)
- Pending NFC Devices (Property of NFC Devices List)

4.2 MyKey Management Inner STM

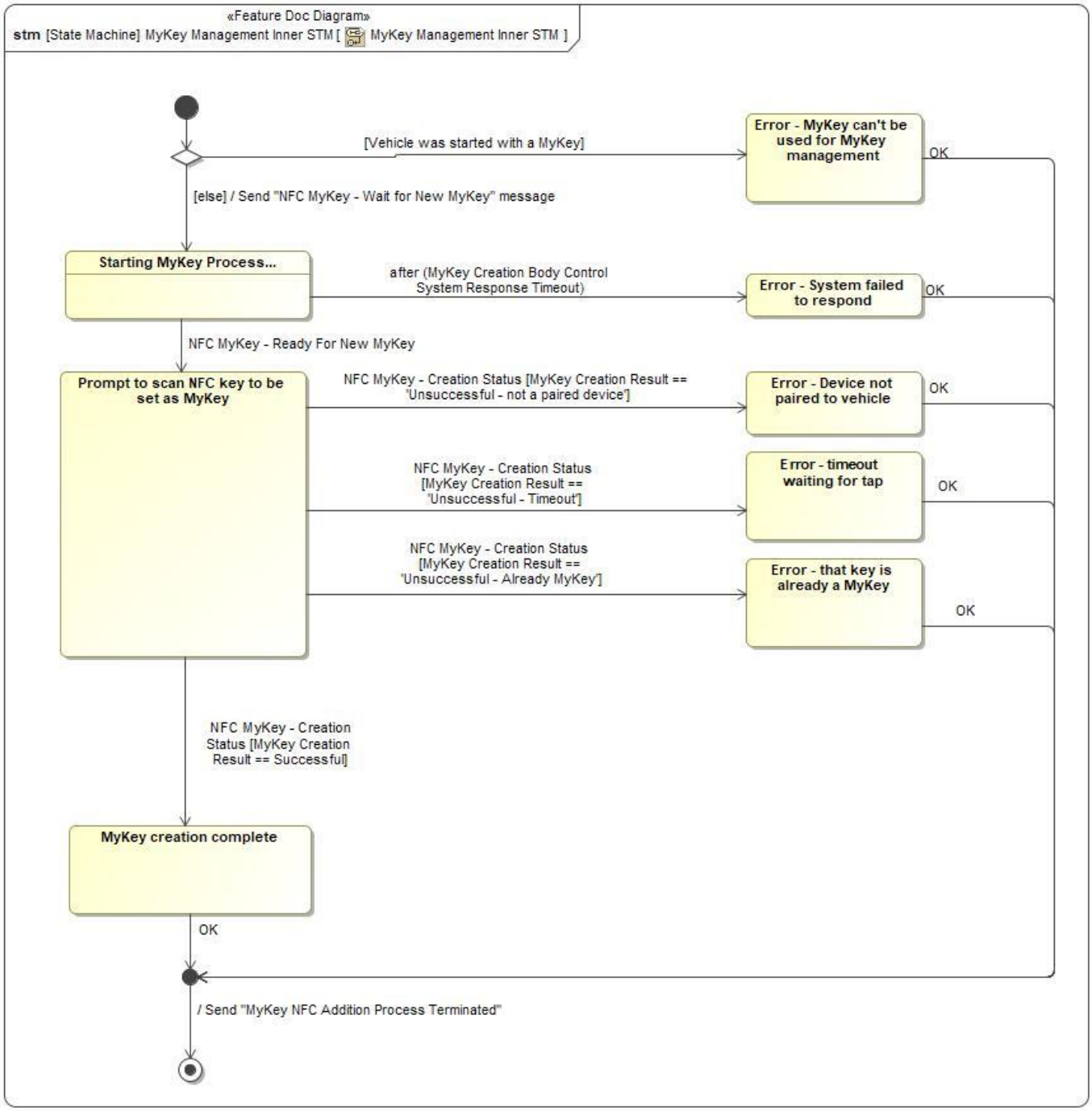


Figure 5: MyKey Management Inner STM

4.2.1 MyKey Management Inner STM Screens

State	Description	Requirements Reference
Error - Device not paired to vehicle		SR NFC MyKey Creation Device not paired error
Error - MyKey can't be used for MyKey management	The vehicle was started using a key with MyKey restrictions. MyKey management is not available. To	SR NFC MyKey Creation not allowed while MyKey in use

	create MyKeys or reset the MyKey system, turn the car off and start it again with a standard key.	
Error - System failed to respond		NFC MyKey Creation System Error timeout
Error - that key is already a MyKey		NFC MyKey Creation Already a MyKey error
Error - timeout waiting for tap		NFC MyKey Creation waiting for Tap timeout
MyKey creation complete		NFC MyKey Creation Flow Success
Prompt to scan NFC key to be set as MyKey		
Starting MyKey Process...	Entry behavior: Start MyKey Process	Initiate NFC MyKey Creation Flow

Table 3: Operation Modes and States on MyKey Management Inner STM

4.2.2 MyKey Management Inner STM requirements

REQ-NFC-ES-180 Initiate NFC MyKey Creation Flow

When the user presses the “Create an NFC MyKey” soft button, the Display System shall initiate the “Create an NFC MyKey” flow by:
- Transmitting an "NFC MyKey – Wait for New MyKey" Request Signal

Rationale: Pressing the "Create an NFC MyKey" Softbutton should initiate the creation flow

REQ-NFC-ES-192 NFC MyKey Creation Flow Success

When the The Display System receives "NFC MyKey Creation Result" Status signal == “Successful” it shall display an NFC Feature related center-stack pop-up which includes:
- Reason text: "MyKey Creation Flow Successful"

Rationale: Notify the user after an NFC Device was successfully updated to be a MyKey

Acceptance Criteria: In-vehicle HMI shall display "MyKey Creation Flow Successful" pop-up when an NFC MyKey is successfully created

REQ-NFC-ES-193 NFC MyKey Creation System Error timeout

If after Starting the MyKey Creation process the Display System does not receive a "NFC MyKey - Ready for New MyKey" signal within "Display MyKey Creation Time" configuration parameter timer of the Display System, it shall exit the “Create an NFC MyKey” flow and
display an NFC Feature related center-stack pop-up which includes:
- Reason text: "Error - System Failed to Respond"

Rationale: MyKey Creation exit path for if there is a system error after initiating the create flow

Acceptance Criteria: Initiating the MyKey Creation process, and inhibiting a response back from the Body Control System will result in cancelling the MyKey Creation flow and displaying a pop-up indicating a system after Creation Time timer has expired

REQ-NFC-ES-194 NFC MyKey Creation Already a MyKey error

If after Starting the MyKey Creation process and having received "NFC MyKey - Ready for New MyKey" signal == "True", the Display System receives an "NFC MyKey - Creation Status" Message with "Mykey Creation Result" signal == "Unsuccessful - already a MyKey" it shall exit the “Create an NFC MyKey” flow and display an NFC Feature related center-stack pop-up which includes:
- Reason text: "Error - Already a MyKey"

Rationale: MyKey Creation should exit if the user scans an existing NFC MyKey during the creation flow

Acceptance Criteria: Scanning an NFC Device that is already a MyKey during the MyKey creation process will terminate the process and display a pop-up indicating key is already a MyKey

REQ-NFC-ES-195 NFC MyKey Creation Device not paired error

If after Starting the MyKey Creation process and having received "NFC MyKey - Ready for New MyKey" signal == "True", the Display System receives an "NFC MyKey - Creation Status" Message with "Mykey Creation Result" signal == "Unsuccessful - Not a paired device" it shall exit the “Create an NFC MyKey” flow and display an NFC Feature related center-stack pop-up which includes:
- Reason text: "Error - Device not paired to vehicle"

Rationale: MyKey Creation should exit if the user scans a device that wasn't previously paired to the vehicle

Acceptance Criteria: Scanning/selecting an unpaired NFC Device during the MyKey flow shall cause the flow to exit and the HMI to display a pop-up stating "Device not paired to vehicle"

REQ-NFC-ES-196 NFC MyKey Creation waiting for Tap timeout

If after Starting the MyKey Creation process and having received "NFC MyKey - Ready for New MyKey" signal == "True", the Display System receives an "NFC MyKey - Creation Status" Message with "Mykey Creation Result" signal == "Unsuccessful – Timeout" it shall exit the “Create an NFC MyKey” flow and display an NFC Feature related center-stack pop-up which includes:
- Reason text: "Error - Timeout waiting for tap"

Rationale: MyKey Creation should exit if the user does not take an action within a specified timeframe after initiating the create flow

Acceptance Criteria: Initiating the MyKey creation process and not scanning an NFC device within MyKey Creation Timer, it shall exit the MyKey create flow and display "error - timeout waiting for tap" message

REQ-NFC-ES-244 NFC MyKey Creation not allowed while MyKey in use

When a user presses the greyed out "Create NFC MyKey" Soft button while the following conditions are true:
- Current MyKey Level == MyKey
The Display System shall not initiate the “Create an NFC MyKey” flow and momentarily indicate that the Create NFC MyKey operation isn't allowed while a MyKey device is in use

*HMI to determine exact verbiage of momentary pop-up

Rationale: MyKey user is not allowed to create additional MyKey devices

4.3 Personal Profiles Linking STM

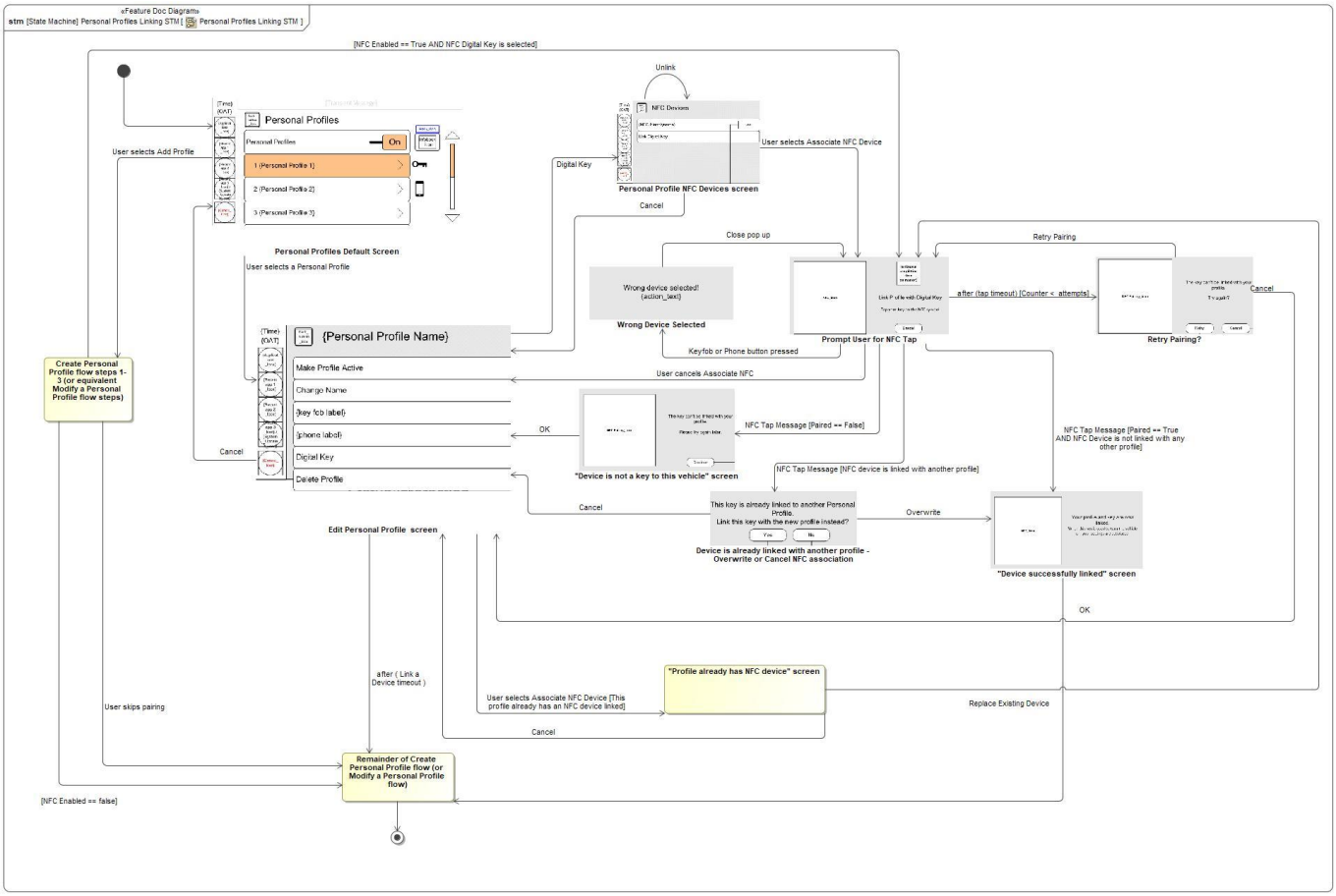


Figure 6: Personal Profiles Linking STM

4.3.1 Personal Profiles Linking STM Screens

State	Description	Requirements Reference
"Device is not a key to this vehicle" screen		invalid NFC device used
"Device successfully linked" screen	Entry behavior: Update Personal Profile Linked Device	Successful NFC Device link to current Personal Profile NFC device already linked to another Personal Profile -ON LINK current NFC to current Personal Profile option
"Profile already has NFC device" screen		Personal Profile already has NFC device Paired Personal Profile already has NFC device Paired ON LINK current NFC to current Personal Profile option Personal Profile already has NFC device Paired ON LINK current NFC to different Personal Profile option NFC Feature enabled on Display system
Create Personal Profile flow steps 1-3 (or equivalent Modify a Personal Profile flow steps)		

Device is already linked with another profile - Overwrite or Cancel NFC association		NFC device already linked to another Personal Profile -ON LINK current NFC to different Personal Profile option
Edit Personal Profile screen		
Personal Profile NFC Devices screen		
Personal Profiles Default Screen		
Prompt User for NFC Tap		
Remainder of Create Personal Profile flow (or Modify a Personal Profile flow)		
Retry Pairing?		
Wrong Device Selected		

Table 4: Operation Modes and States on Personal Profiles Linking STM

4.3.2 Personal Profiles Linking STM requirements

REQ-NFC-ES-181 invalid NFC device used

If after the user has initiated the "Link a device" flow within the Personal Profiles menu, the display system receives an "NFC Tap" message with "Paired" status == False, the Display system shall skip the Profile to NFC Device pairing process and display an NFC Feature related center-stack pop-up which includes:

- Reason text: "Device is not a key to this vehicle"

Rationale: informs user that an invalid NFC device was used to link to a Personal Profile

Acceptance Criteria: HMI exits profile pairing flow and displays dismiss-able pop-up indicating "Device is not a key to this vehicle"

REQ-NFC-ES-190 NFC device already linked to another Personal Profile -ON LINK current NFC to current Personal Profile option

When if the user selects to "overwrite previous pairing" while in the "Link a device" flow within the Personal Profiles Menu, the Display System shall associte the selected profile with the "NFC Tap" message "FESN" value and display an NFC Feature related center-stack pop-up which includes:
- Reason text: "Device successfully paired to profile"

Rationale: Allow USER to link current NFC device to current profile.

Acceptance Criteria: HMI exits profile pairing flow and displays dismiss-able pop-up indicating "Device successfully paired to profile"Target profile updated to indicate new device pairing

REQ-NFC-ES-191 NFC device already linked to another Personal Profile -ON LINK current NFC to different Personal Profile option

When the option "Link a different NFC device to current Personal Profile" is selected in the "Device is already linked with another profile" screen, the Display System shall transition back to "Personal Profile "Link a Device" screen.
Note: the "Personal Profile "Link a Device" screen wording or instructions may differ slightly from original screen, prioritizing requirements detailed in REQ. NFC Personal Profile Pairing process consistency

Rationale: Allow USER to link a different NFC device to current profile.

Acceptance Criteria: Selecting to pair an NFC Device to a different profile shall enable the "Link a device" screen

REQ-NFC-ES-199 Personal Profile already has NFC device Paired

If the user has initiated the "Link a device" flow within the Personal Profiles menu for a Profile that already has an NFC Device associated to it, the Display system shall display an NFC Feature related center-stack pop-up which includes:

- Reason text: "Profile already associated to NFC Device"
- Option to overwrite previous pairing
- Option to skip pairing

Rationale: inform USER that this Personal Profile already has a NFC device linked to it.

Acceptance Criteria: HMI displays dismissable pop-up indication "Profile already associated to NFC Device" with following options:- Option to overwrite previous pairing - Option to skip pairing

REQ-NFC-ES-200 NFC Feature enabled on Display system

The Display System shall support all of the NFC Feature specific functionality while the "NFC Enabled" configuration parameter of the Display System is set to "Enabled"

Acceptance Criteria: NFC related Key Management Menu, MyKey selections, Profile Device Selections, and Centerstack Pop-ups enabled when NFC Enabled is true

REQ-NFC-ES-202 Personal Profile already has NFC device Paired ON LINK current NFC to current Personal Profile option

When the option "Link current NFC Device to current Personal Profile" is selected in the "Profile already has NFC device" screen, the Display System shall sequentially complete the following:
- Remove linkage of the current Personal Profile NFC device value property ESN
- Link the NFC tap message value property ESN to the current selected Personal Profile.
- transition to "Device successfully linked" screen.

Rationale: Allow USER to link current NFC device to current profile.

Acceptance Criteria: HMI exits profile pairing flow and displays dismiss-able pop-up indicating "Device successfully paired to profile"Target profile updated to indicate new device pairing

REQ-NFC-ES-203 Personal Profile already has NFC device Paired ON LINK current NFC to different Personal Profile option

When the option "Link NFC Device to different Personal Profile" is selected in the "Profile already has NFC device" screen, the Display System shall transition back to "Personal Profile "Link a Device" screen.
Note: the "Personal Profile "Link a Device" screen wording or instructions may differ slightly from original screen, prioritizing requirements detailed in REQ. NFC Personal Profile Pairing process consistency

Rationale: Allow USER to link a different NFC device to current profile.

Acceptance Criteria: HMI returns to profile selection screen

REQ-NFC-ES-220 Successful NFC Device link to current Personal Profile

When the CONDITIONS below are met, the Display System shall display the "Device successfully linked " screen after completing the following sequential ACTIONS:
CONDITIONS:
- current screen == "Personal Profile "Link a Device", AND
- NFC tap message signal "Paired" == True, AND
- NFC Tap Message "FESN" signal value not currently paired to any other Personal Profile AND
- Selected Personal Profile not already associated to an NFC device

ACTIONS:
- Link the current NFC tap message value property ESN to the current selected Personal Profile.

Rationale: Allow USER to link current NFC device to current profile.

Acceptance Criteria: HMI exits profile pairing flow and displays dismiss-able pop-up indicating "Device successfully paired to profile"Target profile updated to indicate new device pairing

4.4 Remove NFC Key Inner STM

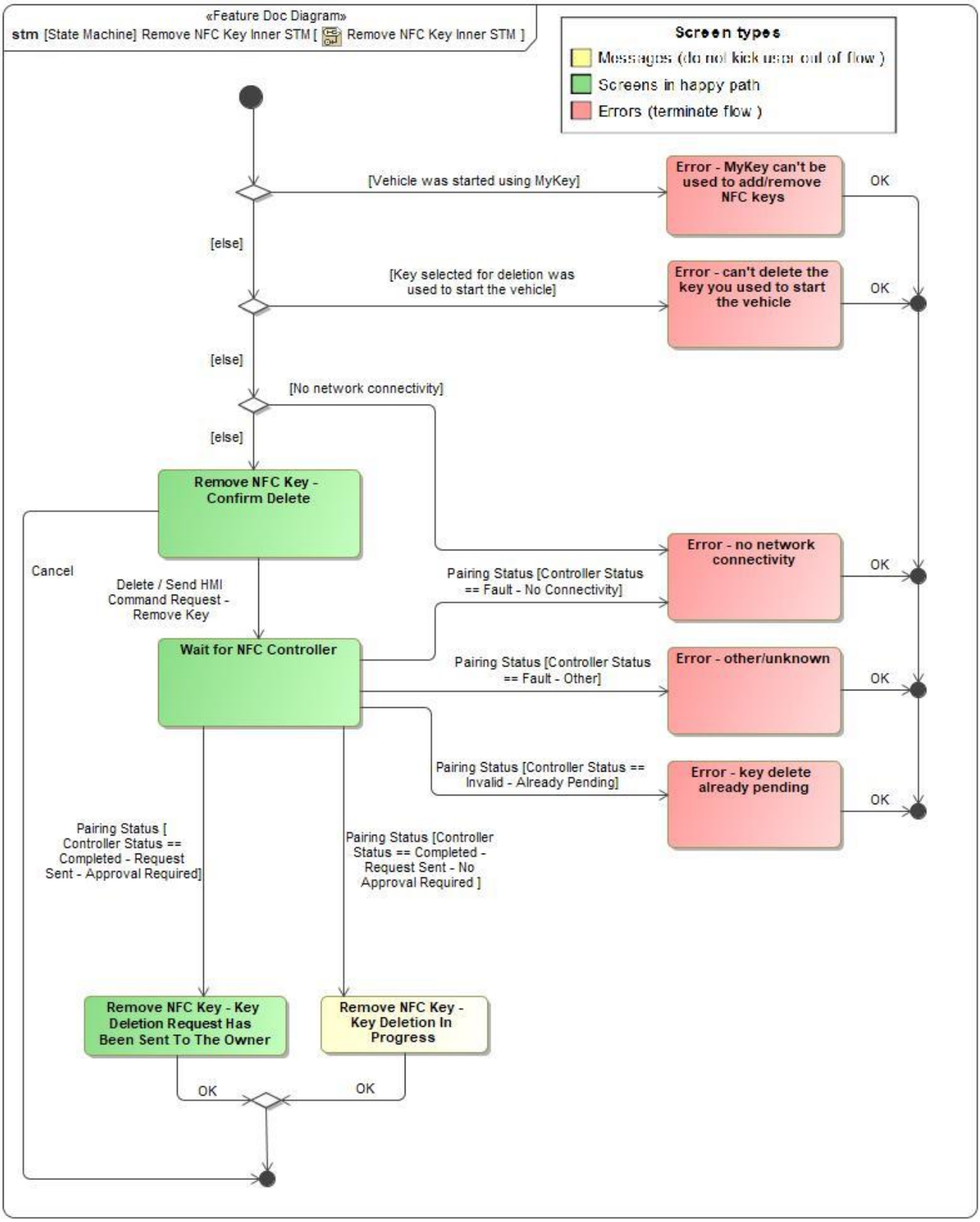


Figure 7: Remove NFC Key Inner STM

4.4.1 Remove NFC Key Inner STM Screens

State	Description	Requirements Reference
Error - can't delete the key you used to start the vehicle	The key that the user selected for deletion is the key that was used to start the vehicle. You can't delete the key you used to start the vehicle. To delete this key, turn the car off and start it with a different key.	Error Screen: Selecting "Delete Key" Button for key used to start the vehicle
Error - key delete already pending		Error screen: Key delete already pending
Error - MyKey can't be used to add/remove NFC keys		Error Screen: Selecting "Delete Key" Button When MyKey is Active Error Screen: Attempting to add or delete a key when MyKey restrictions are active
Error - no network connectivity		Error Screen: Attempting to Add or Delete Keys When There Is No Network Connectivity Display System: Error screen after user confirms NFC Key Delete request
Error - other/unknown		Error screen: Other Error during NFC Card Delete
Remove NFC Key - Confirm Delete	Confirm that the user wants to delete the specified NFC key - it will no longer be able to open or start the vehicle.	Display System: Confirmation Screen when NFC Key Deletion is requested Prompt screen: confirm NFC key pairing deletion - cancel action
Remove NFC Key - Key Deletion In Progress		
Remove NFC Key - Key Deletion Request Has Been Sent To The Owner		Prompt Screen: Key deletion request has been sent to owner Display System: Success screen after user confirms NFC Key Delete request
Wait for NFC Controller		Prompt screen: confirm NFC pairing deletion - actions when confirmed

Table 5: Operation Modes and States on Remove NFC Key Inner STM

4.4.2 Remove NFC Key Inner STM requirements

REQ-NFC-ES-166 Display System: Confirmation Screen when NFC Key Deletion is requested

When the user presses any of the "delete NFC key pairing" buttons/controls in the NFC key management interface, and all of the following are true:

- The vehicle has network connectivity
- The vehicle's modem is authorized
- The key selected for deletion is not the key that started the vehicle
- The key selected for deletion is not a factory key
- The vehicle's ignition is in RUN
- The key that started the vehicle is not a MyKey
- The "NFC Fleet Management Active" configuration parameter of the Center Stack Display System is False

then the Display System shall display a message asking the user to confirm deletion of the NFC pairing.

The message should contain the friendly name and the card FESN of the pairing to be deleted.

Rationale: Requires user to confirm they really wanted to delete an NFC Key.

Acceptance Criteria: Pressing delete button when preconditions are satisfied results in a confirmation prompt being displayed

REQ-NFC-ES-168 Display System: Error screen after user confirms NFC Key Delete request

If either of the following occurs:

- The user presses the "delete key" button for a paired NFC device while the vehicle does not have network connectivity
- While the Display System is displaying the "Wait for NFC Controller" screen in the NFC card delete flow, it receives a Pairing Status message with the "Controller Status" value set to "Fault - No Connectivity"

then the Display System shall display a message indicating that there is no network connectivity, and NFC keys can only be deleted from the vehicle when there is network connectivity. Dismissing this message shall return to the Unified Key Management Screen or the key information screen where the user pressed the delete button.

Rationale: Informs user that request to delete key has failed due to lack of network connectivity or because of a system timeout

Acceptance Criteria: In-vehicle HMI shall not initiate NFC Device Delete request if there is no vehicle connectivity at the time of request

REQ-NFC-ES-169 Prompt screen: confirm NFC pairing deletion - actions when confirmed

If the Display System is displaying the Remove NFC Key - Confirm Delete screen in the NFC card delete flow, and the user presses the Confirm button (or equivalent), the Display System shall:

- Transmit an HMI Command Request message with:
  - the FESN value set or key ID to the Pairing ID of the pairing the user has selected for deletion
  - the Friendly Name value empty/null
  - the Command Type value set to "Delete Pairing"
- Transition to the "Wait for NFC Controller" screen

Rationale: Informs user that request to delete key has been processed

REQ-NFC-ES-170 Display System: Success screen after user confirms NFC Key Delete request

When the Display System is displaying the "Wait for NFC Controller" screen in the NFC key delete flow and it receives a Pairing Status message with the "Controller Status" value set to "Completed - Request Sent - Approval Required", it shall display a message indicating that a request to delete an NFC pairing has been sent to the owner's phone for approval.

The message should indicate that the key is still usable to start and drive the vehicle until the deletion is approved by the owner.

Dismissing the message shall return the Display System to the Unified Key Management screen.

Rationale: Informs user that request to delete key has been sent successfully

Acceptance Criteria: Display System passes through "Wait for NFC Controller" state and displays a success message as above when the vehicle has connectivity

REQ-NFC-ES-175 Error Screen: Attempting to add or delete a key when MyKey restrictions are active

When the key that started the vehicle is a MyKey, and either of the following occurs:

A user presses the disabled "Add NFC Card" button on the Unified Key Management Screen
A user presses the disabled "Remove NFC Key" button (or equivalent) on the Unified Key Management Screen or a key info screen

the Display System shall display a message indicating that NFC pairings and unpairings are not allowed while MyKey restrictions are active.

The message should inform the user that they need to shut off the vehicle and start it with a key that is not a MyKey in order to manage NFC pairings.

Dismissing the message shall return the Display System to the Unified Key Management Screen.

Rationale: This screen informs the user that NFC cards cannot be added to the vehicle when MyKey is active.

Acceptance Criteria: In-vehicle HMI will grey out "Add a Key" and key delete buttons when MyKey is in use; pressing the disabled buttons causes a message to display

REQ-NFC-ES-178 Error Screen: Attempting to Add or Delete Keys When There Is No Network Connectivity

When any of the following occurs:

- The user presses the "Add NFC Card" button on the Unified Key Management Screen and the vehicle has no network connectivity
- The user presses the "Delete NFC Key" button (or equivalent) on the Unified Key Management Screen or a NFC key info screen
- While the HMI is displaying the "Waiting for NFC Controller" screen in the NFC key add or NFC key delete flows, or the "Prompt for NFC card scan" screen in the NFC key add flow, it receives a Pairing Status message with the "Controller Status" value == "Fault - No Connectivity"

then the Display System shall display a message to the user indicating that there is no network connectivity, and NFC cards cannot be added or deleted when there is no network connectivity.

Dismissing this message shall return a user to the Unified Key Management Screen.

Rationale: User guidance when key adds are not allowed

Acceptance Criteria: Pressing "Add a Key" button or any NFC key delete button within in-vehicle HMI shall not start the key pairing process and display a pop-up indicating vehicle has no connectivity

REQ-NFC-ES-234 Error Screen: Selecting "Delete Key" Button When MyKey is Active

When a user presses the greyed out "Delete NFC Key" Soft button while the following conditions are true:
- Current MyKey Level == MyKey

The Display system shall display a momentary pop-up to indicate the NFC Delete operation isnt allowed while a MyKey device is in use

Rationale: This screen informs the user that NFC key cannot be deleted from the vehicle when MyKey is active.

REQ-NFC-ES-243 Error Screen: Selecting "Delete Key" Button for key used to start the vehicle

When a user presses the "Delete Key" button for the key that was used to start the vehicle, the display system shall display a message indicating that the key that was used to start the vehicle cannot be deleted.

The message should instruct the user to start the vehicle with a different key in order to delete the key they are trying to delete.

Dismissing the message shall return the user to the Unified Key Management Screen or the key info screen that was displayed prior to pressing the delete button.

Rationale: This screen informs the user that NFC key cannot be deleted from the vehicle when MyKey is active.

Acceptance Criteria: Pressing the delete button for the starting key causes this message to be displayed; delete flow does not proceed

REQ-NFC-ES-351 Error screen: Key delete already pending

When the Display System is displaying the "Wait for NFC Controller" screen in the NFC key delete flow and it receives a Pairing Status message with the "Controller Status" value set to "Invalid - Already Pending", it shall display a message indicating that a request to delete the key in question has already been sent.

The message should indicate that the user should check the owner's FordPass or Lincoln Way app to approve the deletion request.

Dismissing the message shall return the Display System to the Unified Key Management screen.

Acceptance Criteria: Attempting to delete the same key twice results in this message being displayed the second time

REQ-NFC-ES-352 Error screen: Other Error during NFC Card Delete

When the Display System is displaying the "Wait for NFC Controller" screen in the NFC key delete flow and it receives a Pairing Status message with the "Controller Status" value set to "Fault - Other", it shall display a message indicating that an unknown error prevented the NFC key deletion request from being sent.

Dismissing the message shall return the Display System to the Unified Key Management screen.

REQ-NFC-ES-353 Prompt screen: confirm NFC key pairing deletion - cancel action

When the Display System is displaying the "Remove NFC Key - Confirm Delete" screen, and the user presses the "Cancel" button, the Display System shall return to the Unified Key Management Screen, or the screen that the user was on prior to pressing the delete button, and shall not send an HMI Command Request message.

Acceptance Criteria: Pressing "cancel" in key delete confirmation dialog returns to previous screen without delete request being sent

REQ-NFC-ES-443 Prompt Screen: Key deletion request has been sent to owner

When the Display System is displaying the "Wait for NFC Controller" screen in the NFC key delete flow and it receives a Pairing Status message with the "Controller Status" value set to "Completed - Request Sent - No Approval Needed", it shall display a message indicating that key deletion is in progress.

5 REVISION HISTORY

Revision	Description	Responsible
2020-05-22	Initial Functional Specification release for P708 UPV0	abonnel1, fehsan2, ekarpins
2020-08-24	Updated release for P708 UPV1	abonnel1, fehsan2, ekarpins
2020-12-09	Section 2: Updated "Function Group Description" definition Section 2.1: Added "Center Stack Display System Logical System Behavior" diagram Section 2.2: Logical Properties, previously section 2.1. Section 2.2.1.1: Config Parameters, previously 2.1.1.1. Updated list of Config parameters Section 2.2.1.2: Added list of Runtime Variables Section 2.3: Created Logical System Required. Added requirements to capture feedback align with UX and HMI teams feedback Section 3.1: "Add NFC Key InnerSTM", previously "Display System". Updated State machine diagram for NFC Add flow, require user to scan after entering in friendly name Section 3.1.1: "Add NFC Key InnerSTM States" table added Section 3.1.2: "Add NFC Key InnetSTM Requirements" updated to match NFC Add Flow state machine Section 3.2: "HMI" previously section 3.1 "Display System" Section 3.2.1: "HMI States" table, updated state to requirements mapping Section 3.2.2: "HMI Requirements" previously section 3.2.1 "Display System Requirements", modified/updated requirements for tie-in to Personal Profiles, MyKey, and NFC related HMI screens/pop-ups. Deleted requirements that were pulled in from other systems Section 3.4.1: "Personal Profiles Linking STM States", updated States to requirements mapping Section 3.4.2: "Personal Profiles Linking STM Requirements", requirements cleaned up Section 3.5: "Remove NFC Key Inner STM". Updated State machine diagram for NFC Delete Flow, added missing states/errors Section 3.5.1: "Remove NFC Key Inner STM states", updated States to requirements mapping Section 3.5.2: "Remove NFC Key Inner STM Requirements", requirements updated to match NFC Delete Flow state machine Section 5.1: "Data Dictionary" updated to capture more details and link to implementation level signals/messages	abonnel1, fehsan2, ekarpins
2021-08-06	Updated release for P702MCA MY24 UPV1: • Added screens and flows for NFC Mobile (CCC Digital Key) content. All wireframes/state machines updated. • Added requirements for NFC Mobile (CCC Digital Key) content. NFC Mobile requirements are prefixed with REQ-NFC-DK. These requirements, although new for this version of the specification, are not included in the lists of added requirements below for conciseness. Section 3 “Function Group Description”: • Added “HMI Screens” table describing screens and associated requirements. • Added runtime variables “Ignition On”, “MyKey State”, “Starting Key Type”, “Gear Shift Position”, “Ignition Status”, and “Modem Authorized”.	abonnel1, adelong2, fehsan2, ekarpins, jwolf53, rsepulv6

	• Removed runtime variable “HMI Available”. Section 3.3 “Logical System Requirements”: • Updated REQ-NFC-ES-4 “NFC Card Info Screen” (add mobile content). • Updated REQ-NFC-ES-50 “Master Reset – User Initiation Limitation” (was “Master Reset – MyKey Cannot Initiate”) • Added REQ-NFC-ES-83 “Retail users not allowed to remove Factory Keys” (mistakenly omitted, not new content) • Removed REQ-NFC-ES-85 “NFC User Key not allowed to initiate Master Reset” (redundant) • Updated REQ-NFC-ES-92 “MyKey Users not allowed to add or remove NFC Key” (was “MyKey Users not allowed to add or remove NFC Cards”) • Removed REQ-NFC-ES-135 “Master Reset Screen – User Cards not allowed to initiate Master Reset” (redundant) • Added REQ-NFC-ES-189 “NFC Feature specific pop-up classifications and duration” • Added REQ-NFC-ES-435 “Prompt Screen: No MyKey can pair/change owner device” Section 4.1 “Add NFC key InnerSTM” • Added: REQ-NFC-ES-226 “Sending Request screen – transmit HMI Command Request signal” • Added: REQ-NFC-ES-431 “Friendly name input – requirements” • Added: REQ-NFC-ES-432 “Friendly name input – strip leading and trailing whitespace” • Added: REQ-NFC-ES-433 “Friendly Name input – placeholder/default input” Section 4.3 “Personal Profiles linking STM” • Updated wireframes based on documentation from Personal Profiles/Enhanced Memory feature team • Removed: REQ-NFC-ES-187 “NFC device already linked to another Personal Profile” Section 4.4 “Remove NFC Key Inner STM” • Updated wireframes – add “key deletion in progress” screen • Updated: REQ-NFC-ES-170 “Display System: Success screen after user confirms NFC Key Delete request” • Added: REQ-NFC-ES-443 “Prompt Screen: Key deletion request has been sent to the owner” •	
2021-09-19	**Section 3.3 Logical System Requirements** • *Added*: REQ-NFC-ES-458	abonnel1, adelong2, fehsan2, ekarpins, jwolf53, rsepulv6

6 APPENDIX

6.1 Data Dictionary

6.1.1 Logical Messages

CCC Mobile Pairing Callback

Name	CCC Mobile Pairing Callback
Description	This signal is used in Owner Paring and is sent from the Native App to the Owner Mobile App when the KTS is received. This signal is only received if the KTS is not received by the time CCC Phase 4 is completed.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
result	Callback	This is the result of the callback from the Native App. It contains events that are happening at the Native App.	

Delete Old Owner Key

Name	Delete Old Owner Key
Description	This signal is used in Mobile Key Termination and sent from the Ford Cloud to indicate that someone is trying to pair an owner device, but there is already one paired. This is used because only one owner device can be paired to the vehicle at a time.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Key ID	KeyID	This is the unique identification of the key that is being deleted from the FP/LW.	
Event Type	Termination Event	This is the type of termination that is being requested from FP/LW. This is determined by who/how the key is terminated.	

Device Entered Field

Name	Device Entered Field
Description	To indicate that a device has entered within the detection range of an NFC Reader Antenna
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Location	NFC Location	Whether a device was detected at an interior or exterior reader antenna's field	

AID	AID	Application Identifier - This will determine if the device being scanned at the NFC Reader is a phone that is owner pairing or not, or if it is a card.	

Device Exited Field

Name	Device Exited Field
Description	To indicate that a device has exited the detection range of an NFC Reader after being detected.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Location	NFC_Location	Whether a device has exited the detection range of an interior or exterior reader antenna's field	

Diagnostic Session Request

Name	Diagnostic Session Request
Description	Request from the Service tool to the target system to initiate a diagnositc session
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Session	Diagnostic_Session_Type		

Diagnostic Session Result

Name	Diagnostic Session Result
Description	Result from the target system back to the Service tool, indicating its diagnostic session
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Session	Diagnostic_Session_Type		
Status	Boolean		

Digital Key Data Request

Name	Digital Key Data Request
Description	This message is sent from the Mobile App to the Ford Cloud when the Mobile App needs new key data, but it does not have the most up-to-date data.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Account ID	Account ID	This is the unique account identifier of the account that is requesting the updated key list.	

Digital Key Data Response

Name	Digital Key Data Response
Description	This message is sent from the Ford Cloud to the Mobile App in response to the Digital Key Data Request. This message contains all key data for the requested vehicle.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
NFC Feature Package	NFC Feature Package	This will show if the NFC Feature Package is equipped or not. If it is not and key data is requested, it will notify the user of that.	
friendProfile	userRole		
Key List	Digital Key List		

Digital Key Owner Pairing Progress

Name	Digital Key Owner Pairing Progress
Description	This signal is used in Owner Paring and sent from the NFC Controller to the Center Stack Display (SYNC) to notify them that a pairing has started, is pairing, or finished.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Event	Pairing HMI Event		
Type	Pairing HMI Type		

Enable/Disable NFC Feature

Name	Enable/Disable NFC Feature
Description	This signal is a command to devices in the vehicle to either enable or disable that device's behavior related to the NFC Entry and Starting feature. The device should enable or disable the feature behavior based on the value of the "Enable/Disable" property.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Enable/Disable	Enable/Disable	Whether the feature should be enabled or	

		disabled on the target module	

FactoryCardCANNodeID update

Name	FactoryCardCANNodeID update
Description	CANNodeID tied to NFC Factory Card association on NFC System. Assigned between 801-809
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
CANNodeID	Integer	CAN Node ID value between 801 to 808, reserved for NFC Factory Cards	
FESN	FESN	The Ford Electronic Serial Number for the NFC Card/Device either being added or deleted.	
VehicleData	VIN	Data to identify the target vehicle. Idealy the Vehicle Identification Number of the originating vehicle	

HMI Command Request

Name	HMI Command Request
Description	The message that is sent from the vehicle's Display System to the vehicle's NFC System when a retail user requests an NFC command using the in-vehicle HMI. Causes an "NFC Command Request - Retail" message to be sent to the Cloud Backend System by the NFC System.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Friendly Name	String	In the case of a card add, the user-entered name for the NFC card to be added. In the case of a card delete or a cancel command, null/unpopulated.	
Requested Command Type	HMI Card Request	The action being requested (add, delete, cancel).	
Pairing ID	Pairing ID		
Local ID	Local ID		

Key Deleted Email

Name	Key Deleted Email
Description	This message is used in Mobile Key Termination and sent from the cloud to the Owner Email account to notify them of key deletion.
Realized by	_

Key Deleted Notification

Name	Key Deleted Notification
Description	This message is used in Mobile Key Termination and sent from the cloud to the Owner or Friend Device to notify them of key deletion.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
VIN	VIN		
Friendly Name	String		
Account ID	Account ID		

Key Search Request

Name	Key Search Request
Description	A message sent from the Body Control System to the NFC System to determine whether the NFC system is in the "starting authorized" state. This message is triggered by a number of user actions (pressing brake pedal, opening door, etc).
Realized by	_

Key Search Response

Name	Key Search Response
Description	The message that is sent by the NFC System to the Body Control System in response to a Key Search Request. This reply is sent whether or not the NFC System is in the starting authorized state. This message constitutes starting authorization when the Authorized runtime variable is True.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Authorized	Boolean	Whether the NFC system authorizes starting.	
Authorizing key	Integer	If starting is authorized, the index of the NFC device that authorized starting. If starting is not authorized, undefined.	
Authorizing key type	NFC Key Type	The type of the NFC key that authorized starting (factory key, retail user key, fleet user key).	
Authorized Key Technology	ActivePassiveNull	This is the type of device technology (active or passive) that is currently authorized for the vehicle to drive.	

Key Search Trigger

Name	Key Search Trigger
Description	
Realized by	_

Manufacturing Pairing Event

Name	Manufacturing Pairing Event
Description	A signal emitted by the NFC System each time a manufacturing pairing event occurs. A manufacturing pairing event is when the NFC System attempts to add a new factory card pairing because it is in Factory Pairing Mode and a card is presented. This signal is used to trigger feedback behavior for the assembly technician (e.g., flashing the turn signals, or presenting a message in the cluster).
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Successful	Boolean	Whether the detected NFC key card was paired successfully.	

Master Reset Command

Name	Master Reset Command
Description	The signal that is emitted when a Master Reset event is triggered, whether it was triggered through the in-vehicle HMI or remotely (for fleets). This signal is used by the NFC System to trigger the NFC System's Master Reset behavior.
Realized by	_

Mobile App Approval Request

Name	Mobile App Approval Request
Description	The message that is transmitted from the Cloud Backend System to the Mobile App to prompt the retail owner to approve or deny a request that was created using the in-vehicle HMI.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Card FESN	FESN	The Ford Electronic Serial Number for the NFC Card/Device either being added or deleted.	
Request Type	NFC Command Type	The specific type of action being requested: Adding a Key, Deleting a Key	
Key Friendly Name	String	The user friendly name of the NFC Card/Device either being added or deleted.	
Pairing ID	Pairing ID	Unique pairing ID that is created and maintained on the cloud side to keep track of vehicle to NFC Device pairings.	
Device Type	NFC Device Type	The type of device (Ford NFC key card, CCC mobile device) that is the subject of this request.	
Request Timestamp	Timestamp		

Response Deadline	Timestamp		
VIN	VIN	The VIN of the vehicle that this request applies to.	

Mobile App Approval Response

Name	Mobile App Approval Response
Description	The message sent by the Mobile App that contains the user's decision on a specific approval request.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Approval Response	Retail Owner Approval Status	The approval response a Retail admin - user authorized to the vehicle's modem - can provide in response to receiving requests for adding or deleting NFC devices from their vehicle	
Pairing ID	Pairing ID	The payload ID associated with the specific device that is being either added to or deleted from the vehicle	

Mobile Pairing DK Request

Name	Mobile Pairing DK Request
Description	This message is used in Owner Pairing to send information from the Owner Mobile App to the Ford Cloud to start owner pairing. The information contained in this message is everything needed to start the owner pairing process on the Ford Cloud and create verifiers.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Friendly Name	String		
Request ID	Request ID		
VIN	VIN		
DK Version	DK Version		
Device ID	Device ID		
Account ID	Account ID		

Mobile Pairing DK Response

Name	Mobile Pairing DK Response
Description	This message is used in Owner Pairing to send information from the Ford Cloud to the Mobile App in response to its pairing request. This signal contains an SPAKE password to be used when pairing the owner device.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Pairing Password	Pairing Password		
requestID_Resp	Request ID		

Modem Deauthorization

Name	Modem Deauthorization
Description	We expect this signal to be sent when the vehicle's modem becomes deauthorized for any reason.
Realized by	_

NFC Cloud Event

Name	NFC Cloud Event
Description	This signal is transmitted from the NFC System to the Cloud Backend System when one of a number of different events occur on the vehicle. It is used to update the state of the Cloud Backend System to match the on-vehicle state, confirm the completion of remote commands, and log failure events for later analysis.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Event Type	NFC Event Type	The pass or fail status of the specific add/delete/master reset/modem deauth/factory key pairing action the vehicle took	
Associated FESN	FESN	If there is a specific NFC key card FESN associated with the NFC event that occurred, this field contains that FESN.	
Factory Pairing Node ID	Integer	If the event related to an NFC factory card pairing, the virtual CAN node ID assigned to that factory pairing.	
Pairing ID	Pairing ID	Unique ID generated tied to an instance of vehicle to device pairing.	

NFC Cluster Message

Name	NFC Cluster Message
Description	Message sent from the Body Control System to the Driver Information System that indicates which NFC-specific driver warning message should be displayed.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Indication	NFC Cluster Message	Which message should be displayed on the cluster.	

NFC Command

Name	NFC Command
Description	This message is transmitted from the Cloud Backend System to the NFC System to cause a command to be executed on the NFC System.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Command type	NFC_Command_Type	The specific command that is being issued to the NFC System. Always required.	
Command data	Command_Data	The specific data required to complete the requested add/delete command	
Command origin	Command_Origin	Whether the command originated from the vehicle, the fleet management system or a service tool	

NFC Command Request - Fleet

Name	NFC Command Request - Fleet
Description	The message that is sent from the fleet management portal to the NFC Cloud Backend when a fleet manager or other fleet admin requests a command be issued to a fleet-managed NFC vehicle.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
FESN	FESN	The Ford Electronic Serial Number for the NFC Card/Device either being added or deleted. N/A for Enable or Disable requests	
Friendly Name	String	The Friendly Name of the NFC Card/Device either being added or deleted. N/A for Enable or Disable requests	
Command type	NFC_Command_Type	The specific type of action being requested: Adding a Key, Deleting a Key, Disabling NFC feature on target module, Enabling NFC Feature on target module	
VIN	VIN	The Vehicle Identification Number of the vehicle the selected command is being requested for	
Pairing Type	NFC Key Type	The Type of card that is being request for the command.	

NFC Command Request - Retail

Name	NFC Command Request - Retail
Description	The message that is sent from a vehicle to the NFC Cloud Backend when a retail user requests an NFC command using the in-vehicle HMI.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Local ID	Local ID	Vehicle to NFC Device pairing ID that is generated by the vehicle at the time of a Retail NFC Device Add request. It is maintained until either the request is completed, rejected, or timed out.	
Pairing ID	Pairing ID	The Ford Electronic Serial Number for the NFC Card/Device either being added or deleted.	
Command type	NFC Command Type	The add, delete, enable or disable command being requested	
Friendly Name	String	The user selected name for their NFC Device	
Key Trusted	Boolean		
Device Type	NFC Device Type		

NFC Device Detected

Name	NFC Device Detected
Description	Updated and sent when an NFC Device is detected at a Reader
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Location	NFC Location	Whether an NFC Device was detected at an interior or exterior reader	
Device Type	NFC Device Type	The device type is defined by the authentication protocol supported by the device. Ford NFC Cards are devices that support the Ford-specific NFC authentication protocol.	

NFC Devices List

Name	NFC Devices List
Description	Carries the information used to populate the in-vehicle key management screens from the NFC System to the Display System. Sent upon request from the Display System.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By

Pending NFC Devices	–	Pairing requests (add or delete) that have been placed through the in-vehicle HMI and transmitted to the cloud backend, but not yet approved.	
Active NFC Devices	–	Completed pairings that are active on the vehicle.	
Additional Key Storage Available	–	Whether or not the NFC Controller has capacity to store one or more additional NFC device pairings.	
Maximum Pairings	–	The value of the "Maximum Pairings" runtime variable on the NFC Controller.	
Fleet Management Active	–	Whether the NFC system is currently subscribed to (and being managed by) the fleet NFC management feature.	

NFC Local Event

Name	NFC Local Event
Description	This is emitted by the NFC system whenever a valid command is received by the system, after the NFC System finishes executing the command. A valid command is one that is syntactically correct and has a valid signature from Ford. For example, this signal is emitted during the process for creating a new NFC key card pairing, when the actual pairing command is received and executed by the NFC system. Multiple systems on the vehicle consume this message to trigger behaviors when key changes occur: for example, when a key is added to the vehicle, the HMI system uses this signal to trigger a confirmation pop-up, and the Body Control System uses this signal as a trigger to clear the associated MyKey table entry.
Realized by	–

Parameters/Owned Signals

Name	Type	Description	Realized By
Command Type	NFC Command Type	The type of command that was completed (or not completed).	
Outcome	Pairing Request Outcome	The result of the pairing request - whether it was approved, denied, timed out, etc.	
Key Index	Integer	If the command relates to a specific key in the NFC system, this property indicates the NFC key index of that key.	
FESN	FESN	If the command relates to a specific NFC key card, the FESN of that key card. Undefined otherwise.	

NFC MyKey - Creation Status

Name	NFC MyKey - Creation Status
Description	Transmitted from the Body Control System to the Display System to provide feedback on the state of the Body Control System during a MyKey creation operation.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
NFC MyKey Creation Status	NFC MyKey Creation Result	A signal from the Body Control System indicating the status of a MyKey creation operation.	

NFC MyKey - Ready For New MyKey

Name	NFC MyKey - Ready For New MyKey
Description	This signal is sent from the Body Control System to the HMI system to indicate that the request for MyKey creation was received, and the Body Control System will make the next scanned NFC device a MyKey.
Realized by	_

NFC MyKey - Wait for New MyKey

Name	NFC MyKey - Wait for New MyKey
Description	This signal is sent from the HMI system to the Body Control System when the user requests MyKey creation. The signal indicates that the Body Control System should make the next NFC device scanned a MyKey.
Realized by	_

NFC Service Request

Name	NFC Service Request
Description	
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
CommandType	NFC Command Type	The specific type of action being requested: Adding a Key, Deleting a Key, Requesting a Key List, Clearing All Keys, Restoring Keys	
VIN	VIN	Data to identify the target vehicle. Typically just the Vehicle Identification Number of the target vehicle	
FESN	FESN	8 Byte Ford Electronic Serial Number assigned to an NFC Card	
KeyType	NFC Key Type	The categories of keys that can exist in the NFC System; currently limited	

		to Factory, Retail User, or Fleet User	
Friendly Name	String	Max 60 character string used for assigning a "friendly name" to the NFC Card	
Pairing ID	Pairing ID	Unique ID generated at the instance of a vehicle to device pairing, generated by the vehicle and stored within the vehicle and NFC Cloud	

NFC Service Response

Name	NFC Service Response
Description	Transmitted by NFC Cloud Backend in response to receiving NFC Service Request. Contains the Status, and when application, the payload that needs to be delivered to the NFC System in order to complete the request.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Command Type	NFC Command Type	The specific type of action being requested: Adding a Key, Deleting a Key, Requesting a Key List, Clearing All Keys, Restoring Keys	
Command Data	Command Data	The Data required to complete the "Command Type" action being requested of the NFC System	
Command Origin	Command Origin	Indicate whether the command was initiated by a Retail User, the Fleet system, or a service tool	
VIN	VIN	Data to identify the target vehicle, typically just the VIN	
Status	NFC Service Request Status	Indicate whether a NFC Service Request was accepted or rejected for failing a specific conditions(s)	

NFC Service Tool Request

Name	NFC Service Tool Request
Description	
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
CommandType	NFC Command Type	The specific type of action being requested: Adding a Key, Deleting a Key, Requesting a Key List, Clearing All Keys, Restoring Keys	

VehicleData	VIN	Data to identify the target vehicle. Typically just the Vehicle Identification Number of the target vehicle	
TechnicianCredentials	Credentials	Service technician specific credentials used by the Service Cloud Backend to authorize the service technician to request specific data/operations	
FESN	FESN	8 Byte Ford Electronic Serial Number assigned to an NFC Card	
KeyType	NFC Key Type	The categories of keys that can exist in the NFC System; currently limited to Factory, Retail User, or Fleet User	
Friendly Name	String	Max 60 character string used for assigning a "friendly name" to the NFC Card	
Pairing ID	Pairing ID		

NFC Tap Message

Name	NFC Tap Message
Description	This message is emitted by the NFC system every time a transaction is completed with any compatible NFC device (Ford NFC key card or CCC-compliant smart device). This includes non-authorized devices - scanning a device that is not paired with the vehicle will still generate an NFC Tap. This message is consumed by multiple systems in the vehicle to trigger behaviors when an NFC device is tapped. For example, the Body Control System uses this message to trigger vehicle locking/unlocking on an exterior device tap.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Paired	Boolean	Whether the device that was scanned is authorized to this vehicle (i.e., it is paired). True if the device was authorized.	
Tap Duration	NFC Tap Duration	Whether the user performed a short tap or a long tap. A short tap occurs whenever an NFC device was held at the reader for any duration long enough to perform a transaction. A separate NFC Tap message is emitted with Tap Duration = Long Tap if the user continues to hold the device at the reader for longer than the long tap threshold (a second or two).	

Location	NFC Location	The location of the NFC reader where the tap event occurred.	
Key Index	Integer	The internal index of the NFC key that was tapped, if that key was authorized to the vehicle. If the key was not authorized, this value is undefined.	

New Sharing Session Data

Name	**New Sharing Session Data**
Description	This message is used in Key Sharing to send information from the Owner Mobile App to the Ford Cloud. This information includes data that is needed to share the sharing session with the friend device.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
sharingSessionUrl	String		
PIN	PIN		
friendEmail	String		

Pairing Status

Name	**Pairing Status**
Description	The status of a specific NFC Card to vehicle pairing request
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Controller status	Card Pairing Status		

Pin Verification

Name	**Pin Verification**
Description	This message is used in Key Sharing to send information from the Friend Mobile App to the Ford Cloud. It contains the PIN that the friend inputted to verify that it matches the PIN that was created.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Friend PIN	PIN		
Session ID	Session ID		

Request NFC Devices List

Name	**Request NFC Devices List**

Description	A message sent from the Display System to the NFC Controller to request that the NFC Controller transmit a list of active and pending key pairings.
Realized by	_

Retail User Approval Result

Name	**Retail User Approval Result**
Description	This message is sent from the Cloud Backend System to the vehicle to notify the vehicle of the result of a previously requested NFC command. The message is only transmitted if the request has failed, timed out, or been denied -- if the request is approved, the vehicle is notified with an NFC Command Message.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Request Status	Retail_Owner_Approval_Status	The state of the specified approval request.	
Payload ID	_		
Local ID	Local ID	The Local ID originally generated by the vehicle and sent with the original command request. Used by the vehicle to correlate requests with replies.	
Reserved Fields	_		

RoutineControl

Name	**RoutineControl**
Description	Transmitted by the service tool to the target system (i.e. NFC system) requesting it to run a specific diagnostic routine
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
RoutineID	Routine Id	Specific Routine ID being requested by the service tool to be run on the target system	
RoutineData	Routine_Data	Data required to execute a specific routine	

RoutineControlResult

Name	**RoutineControlResult**
Description	Response back from the target module to the service tool after it receives a RoutineControl request
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
RoutineID	Routine Id	Specific Routine ID being requested by the service	

		tool to be run on the target system	
Result	Routine_Result	Indicate whether the routine was able to complete or not	

Secure Access Key Request

Name	Secure Access Key Request
Description	Request sent up from the Service tool to the Service Cloud Backend for a specific module's unlock key
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Technician Credentials	Credentials	Service technician specific credentials used by the Service Cloud Backend to authorize the service technician to request specific data/operations	
Module Data	Module_Data	Module specific DID, Configuration, and diagnostic specific data (as contained with part 2 spec)	
Vehicle Data	VIN	Data to identify the target vehicle. Typically just the Vehicle Identification Number of the target vehicle	

Secure Access Key Result

Name	Secure Access Key Result
Description	Response returned to the Service tool from the Service cloud backend containing a specific module's unlock key
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Result	Boolean	Indicate whether the secure access key request was accepted or rejected by the NFC Service Cloud	
Data	Module_Unlock Key	Data that includes the target module's 12 fixed byte security key	

Secure Access Result

Name	Secure Access Result
Description	Response from the target system back to the service indicating whether it accepted the lock/unlock request and the current lock status of the system
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Result	Boolean	Indicate whether the target module accepted the Security Access Request/data	
Module Lock Status	Module Lock Status	Indicate whether the target module is locked or unlocked (diagnostics POV)	

Security Access Request

Name	Security Access Request
Description	Request from the service tool to the target system request it to be unlocked.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Request	Module Lock Status	Request to lock or unlock the target module	
Request Data	Module Unlock Key	Data that includes the target module's 12 fixed byte security key	

Server Pairing DK Request

Name	Server Pairing DK Request
Description	This message is used in Owner Pairing and sent from the Ford Cloud to the NFC Controller. This message contains information in order to initiate owner pairing on the NFC Controller, including the verifiers.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Friendly Name	String	reused NfcCommand "keyname" property	
Verifiers	Verifiers	- L; salt; other?	
Key Registration Material	Key Registration Material	- this needs to be defined by cyber security	
Request ID	Request ID	- should this be Pairing ID? NO.	

Server Pairing DK Response

Name	Server Pairing DK Response
Description	This message is used in Owner Pairing and sent from the Ford Cloud to NFC Controller in response to the Server Pairing DK Request. This message contains information verify that the verifiers are properly stored and the vehicle is ready to continue pairing.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By

requestStatus	Pairing_Response	do we add an enumeration to NFCinfo_Rsp_event_ET?	
requestID	Request ID	this might be pairing ID instead of request ID.	

Sharing Invitation

Name	Sharing Invitation
Description	This message is used in Key Sharing and sent from the Cloud to the Friend Mobile App. This message contains information about the Sharing Session to continue Key Sharing and notify the friend a key is being shared with them.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
sessionID	_		
ownerAccountName	String		

Sharing Session URL

Name	Sharing Session URL
Description	This message is used in Key Sharing and sent from the Ford Cloud to the Friend Mobile App. This message contains the URL needed to continue Key Sharing.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Sharing Session Url	String		

Start Button Press

Name	Start Button Press
Description	This signal is emitted by some part of the vehicle whenever the START/STOP button is pressed by a user.
Realized by	_

Starting Authorized Status Indication

Name	Starting Authorized Status Indication
Description	This message is continuously emitted by the NFC system, and indicates whether the NFC System is in the "starting authorized" state, and if so how much time remains until that authorization expires. It is consumed by the Body System in order to determine whether the "key not found" or "ready to start" cluster messages should be displayed.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Time Remaining	Boolean	The number of seconds remaining until the NFC System exits the Starting Authorized state, if it is	

		authorized, or zero otherwise.	

Starting Key Information

Name	Starting Key Information
Description	A signal continuously transmitted by the Body Control System with information about the key that started the vehicle.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Starting Key Source	Starting Authorization Source	Whether a digital key, BLE-PaaK, Keyfob, or *reserved* device was used to start the vehicle	
Starting Key Index	Integer	The specific key index (used for managing MyKey restrictions) of the key used to start the vehicle	
Starting Key Type	NFC Key Type	If the starting key is a User Key, Factory Key, or Neither (applicable for all non-Digital Key devices)	

Trigger Deauthorization

Name	Trigger Deauthorization
Description	Trigger Deauthorization is a signal sent from the Body Control System to the NFC System to cause the NFC System to exit the Starting Authorized state when either of the follow conditions occur: - A vehicle is started - An exterior door lock occurs
Realized by	_

Trigger Reauthorization

Name	Trigger Reauthorization
Description	Message is updated and sent to reauthorize a device on system wake-up, if it had been left on the reader prior to wake-up
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Location	NFC Location	Whether the device was detected at an Interior or Exterior reader	

Vehicle Cluster Message

Name	Vehicle Cluster Message
Description	Existing message sent from the Body Control System to the Driver Information System that causes specific warning messages to be displayed on the cluster.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Indication	_	Which message should be displayed on the cluster.	

Write Data Response

Name	Write Data Response
Description	Response from the target system back to the service tool to indicate whether a specific write/update for a specific data identifiers value was completed.
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Data Id	Module Data Identifier	Specific Data Identifier on the target system	
Data Value	Module Data	Specific value of a Data Identifier on the target system	
Result	Boolean	Whether the target system successfully updated its Data Identifier with the Data Value provided through the Write Data by ID signal	

Write Data by ID

Name	Write Data by ID
Description	Request to write/update a specific data identifiers value, sent by the service tool to the target system
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
Data Id	Module Data Identifier	Specific Data Identifier on the target system	
Data Value	Module Data	Specific value of a Data Identifier on the target system	

test

Name	test
Description	
Realized by	_

Parameters/Owned Signals

Name	Type	Description	Realized By
tte	_		
ttse	Verifiers		

6.1.2 Logical Parameters

MyKey Creation Body Control System Response Timeout

Parameter Name	MyKey Creation Body Control System Response Timeout
Description	When the user triggers the MyKey creation flow, and after the Display System sends the message initiating the MyKey creation process on the BCM, the duration that the Display System will wait for a response from the BCM before aborting and displaying an error.
Owner	Center Stack Display System
Type	period duration
Implementation Element	

NFC Card Add NFC Controller Response Timeout

Parameter Name	NFC Card Add NFC Controller Response Timeout
Description	The maximum duration that the Center Stack Display System will wait for a response from the NFC Controller after it sends an HMI Command Request. If no response is received, the Center Stack Display System will display an error.
Owner	Center Stack Display System
Type	period duration
Implementation Element	

6.1.3 Logical Data Types (encodings)

AID

The AID that the device is talking to during an NFC transaction.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
FordAID	This AID is used when a Ford NFC Card enters the field.
cccFramework	This AID is used when a CCC-complaint device is in a pairing state enters the field. This is used exclusively in owner pairing when setting up a device.
cccApplet	This AID is used when a CCC-complaint device enters the field and the device is not in pairing. This will be used most frequently with CCC devices.

Account ID

This is the unique identifier for the users account.

Authenticated DK Record

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Transaction Result	
Digital Key Record	

Build config

Whether a particular vehicle was ordered by a fleet using their FIN code ("fleet" value).

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Retail	The vehicle was not built with a FIN code.
Fleet	The vehicle was built with a FIN code assigned to it.

CCC Specification

Refer to the CCC Specification for more information.

Callback

The callback from the Native App to the Mobile App of the status of owner pairing.

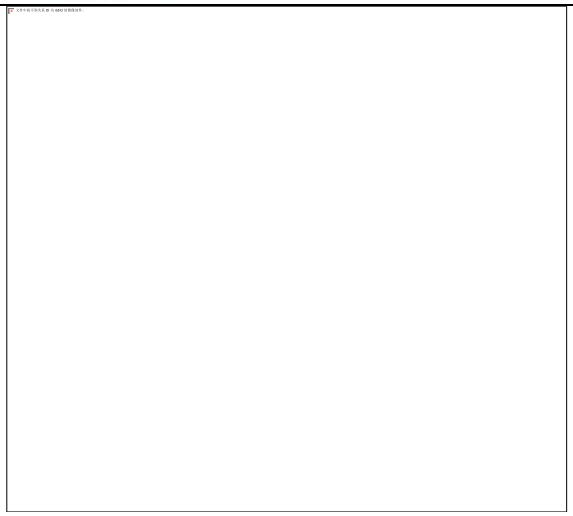
Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Paired	This is called when the KTS has properly been saved by the Naive App and the Owner Key is ready for used.
Waiting KTS	This is called then the KTS Timeout has been reached, but the KTS is still not present.
Recieved KTS	This is called when the KTS is received after the KTS Timeout has already been met. This enumeration shall only be used if Waiting KTS was used.

Card Pairing Record

Card Pairing Record describes the information that is saved in the NFC System for each NFC Key Card pairing (Not Phone Keys) that is created. Each record for a NFC Card contains all of the information listed here, along with the Local Pairing Record (as shown in image below). Local Pairing Record has information that is shared among Phone and Card pairing records.



Note: Please see Data Type in this specification for the most up to date information as this image may be out of date.

Properties of Value Types

Property	Property Description
Card Certificate	
FESN	The FESN of the paired device, if the paired device is a Ford NFC Access Card.
Pairing ID	
Key Type	
Friendly Name	
Factory Card Node ID	

Card Pairing Status

The possible values of the "Controller Status" value in the Card Pairing Status message sent from the NFC System to the Display System during card pairing request creation.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Waiting for Card Tap	The add request has been received, and NFAM is waiting for the user to scan the card that they want to pair.
Fault - No Connectivity	The add or delete request cannot be accepted because there is no network connectivity.
Completed - Request Sent - Approval Required	The NFC Controller has received the user input and successfully transmitted the request to the cloud. An administrator of the vehicle will need to approve the request before it is completed.
Fault - Timed Out	The add request is rejected because no NFC card was scanned before the timeout expired.
Idle	The NFC Controller is not in any pairing request creation process.
Fault - No Capacity	The add request cannot be accepted because there is not capacity on the NFC Controller to store another card pairing. (For the purposes of this determination, pending pairing requests count against the maximum number of pairings.)
Fault - Other	The add or delete request cannot be accepted or completed because of some error that does not fall into another category.
Invalid - Already Pending	The last scanned card cannot be the subject of the add request because an add/delete request is already outstanding for this card. NFAM will continue listening for unpaired card scans.

Invalid - Already Paired	The last scanned card cannot be the subject of the add request because it is already paired with the vehicle. NFAM will continue listening for unpaired card scans.
Fault - Not Paired	The last scanned card cannot be the subject of the delete request because it isnt currently paired to the vehicle/NFAM.
Completed - Request Sent - No Approval Required	The NFC Controller has received the user input and successfully transmitted the request to the cloud. It will be processed and executed without further action.

Command Origin

The entity that caused an NFC command to be issued.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Service tool	A service tool with NFC service functions.
Fleet management service	The fleet web management interface, or a 3rd-party interface that has been granted API access to the fleet web management interface.
Retail user	A retail user, through the vehicle's built-in HMI.

Credentials

The identifying credentials that a service technician uses to log in to the Ford service tool.

DK Action

This is the action that someone wants to perform against a key as defined by 'Action for ManageKey' in Section 17 in the CCC Specification. . We are currently not supporting Suspend/Resume.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
TERMINATE	This is called when a digital key has been selected to be terminated.
SUSPEND	This is used when a digital key has been selected to be suspended. NOTE: Ford is not implementing suspend/resume at this time
RESUME	This is used when a digital key has been selected to be resumed. NOTE: Ford is not implementing suspend/resume at this time

DK Request Data

Data that is needed when a request is made for a digital key.

Properties of Value Types

Property	Property Description
ownerName	
accountID	
dkReleaseVersion	
VIN	
requestID	

DK Version

Version of digital key being used on the vehicle.

Device ID

This is the unique identifier for the specified device.

Device Type

The device that is present during an NFC transaction as defined by Section 17 in the CCC Specification.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Phone	This is used when a CCC-Compliment Phone is detected on the NFC Reader.
Watch	This is used when a CCC-Compliment Watch is detected on the NFC Reader.
Other	This is used when any other CCC-Compliment device is detected on the NFC Reader.

Diagnostic Session Type

Indicate the type of diagnostic session being requested/active

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Default Session	Default session is active
Extended Session	Extended Diagnositcs session is active
N/A	N/A

Digital Key List

This is a list of all digital keys paired to the specified vehicle.

Digital Key Notification Event

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Pairing Successful	A key pairing has been created on the vehicle (the vehicle has confirmed it was successfully created).
Unpairing Successful	A key pairing has been removed from the vehicle (the vehicle has confirmed it was successfully removed).

Pairing Unsuccessful - Vehicle Unreachable	A key pairing could not be created on the vehicle as requested, because the vehicle was offline or unreachable for longer than the maximum retry time. The pairing will not be created.
Unpairing Unsuccessful - Vehicle Unreachable	A key pairing could not be deleted from the vehicle as requested, because the vehicle was offline or unreachable for longer than the maximum retry time. The pairing will not be deleted.
Pairing Unsuccessful - Other	A key pairing could not be added to the vehicle as requested, because of some error other than a connectivity issue. The pairing will not be added.
Unpairing Unsuccessful - Other	A key pairing could not be deleted to the vehicle as requested, because of some error other than a connectivity issue. The pairing will not be deleted.

Digital Key Record

Record of all digital key information on the vehicle.

Properties of Value Types

Property	Property Description
Moblile Key Status	
Vehicle Key Status	
Key Type	
VIN	

Digital Key Terminatiom Record

Record of all digital key that are being terminated on the vehicle.

Digital Key Type

This shows the type of the key on the vehicle as defined by Section 17 in the CCC Specification.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
OWNER	The device is an owner device.
SHARED	The device is a shared/friend device.

Door Lock Status

The status of a vehicle's door locks.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
All Locked	All vehicle doors are locked
Driver Door Unlocked	The last command issued to the vehicle's power door locks was to unlock the driver door.
All Double Locked	The last command sent to the vehicle's electric door locks was to double-lock all of the doors.
All Unlocked	All vehicle doors are unlocked

Enable/Disable

Whether the feature should be enabled or disabled.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Enable	The feature should be enabled.
Disable	The feature should be disabled.

Event Type

The type of event that is being requested for a Digital Key as defined by Section 17 in the CCC Specification.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
IN_TERMINATION	When owner or shared key is being terminated from lo-cal/remote source, this notifi-cation is sent from the Vehi-cle OEM Server to owner or friend Device OEM Server. Digital Key is not terminated yet.
SUSPENDED	NOT SUPPORTED at MVP - When the vehicle suspends owner or shared key, this notification is sent from the Vehicle OEM Server to owner or friend Device OEM Server. Digital Key is suspended.
RESUMED	NOT SUPPORTED at MVP - When the vehicle resumes the owner or shared key, this notification is sent from the Vehicle OEM Server to owner or friend Device OEM Server. Digital Key is resumed.
SHARED_KEY_IN_TERMINATION	When shared key is being terminated from local/remote source, this notification is sent from the Vehicle OEM Server to the owner Device OEM Server. Digital Key is not terminated yet.
SHARED_KEY_TERMINATED	When shared key is terminated (after fade-out period), this notification is sent from the Vehicle OEM Server to the owner Device OEM Server. Digital Key is terminated.
SHARED_KEY_SUSPENDED	NOT SUPPORTED at MVP - When the vehicle suspends a shared key, this notification is sent from the Vehicle OEM Server to the owner Device OEM Server. Shared key is suspended
SHARED_KEY_RESUMED	NOT SUPPORTED at MVP - When the vehicle resumes a shared key, this notification is sent from the Vehicle OEM Server to the owner Device OEM Server. Shared key is resumed.
RESUMING	NOT SUPPORTED at MVP - When the vehicle is resuming all access, this notification is sent to all devices with this Digital Key for the vehicle. Digital Key is not yet resumed on the vehicle.
SHARED_KEY_ADDED	When a shared key has been successfully activated (key is in status “active”), this notification is sent from the Vehicle OEM Server to the owner Device OEM Server.
SUBSCRIPTION_-CHANGED	When Digital Key service subscription changes in Vehicle OEM Server, this notification is sent from the Vehicle OEM Server to owner or friend Device OEM Server. This may occur, e.g., when the Digital Key service is renewed.
SHARING_PASSWORD_REQUIRED	NOT SUPPORTED - When the policy for the sharing password changes in Vehicle OEM Server, this notification is sent from the Vehicle OEM Server to owner or friend Device OEM Server.

SHARING_INITIATED	When owner starts cross-platform key sharing, this notification is sent from Vehicle OEM Server to owner Device OEM Server after friend device redeems sharing session.
SHARING_CANCELLED	this notification is sent from Vehicle OEM Server to owner Device OEM Server or friend Device OEM Server after owner or friend device cancelled cross platform sharing session.
SHARING_TIMEOUT	this notification is sent from Vehicle OEM Server to owner Device OEM Server and friend Device OEM Server if sharing session is neither redeemed nor cancelled after a timeout. The value of timeout is Vehicle OEM Server specific.
ENTITLEMENTS_UPDATED	When entitlements supported by the vehicle are updated in the Vehicle OEM Server and vehicle. These entitlements are then available to the owner for future key sharing operations; existing shared keys are not affected
UI_ELEMENTS_UPDATED	When UI elements such as model is updated in Vehicle OEM Server and propagated to device for existing Digital Key.
VEHICLE_ATTESTATION	NOT SUPPORTED - When vehicle transmits an attestation to the owner device in case a friend enters a correct sharing password in the vehicle. Implementation of this event type is optional for device OEM.

FESN

A Ford Electronic Serial Number.

Friend Event Notification Status

The type of notification that is sent to the Friend Device when specified events occur.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
n/s	
in_termination	

Friend Profile

The key access that the owner permits the friend to have with their shared key.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Unlock and Drive	This is used when the owner selects the profile level of the friend to be Run and Drive.
Restricted Driving	This is used when the owner selects the profile level of the friend to be Restricted Driving.

HMI Card Request

Type for command requests made from the Display System to the NFC Controller.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Add Card	Requests an NFC pairing be added.
Delete Card	Requests an NFC pairing be deleted.
Cancel Request	Exits the add-card flow before the request is sent to the backend. Not applicable to card delete operation.

Ignition Status

The state of the vehicle's ignition.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Off	Vehicle ignition is OFF
Run/Start	Vehicle ignition is in Run/Start (Run position after engine has been started)
Accessory	Vehicle ignition is in Accessory (or Run position without engine started)

Key Registration Material

Data required when key is in the process of being registered.

Key Status

This shows the status of the specified key.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Unpaired	This status of the key is unpaired.
Pairing	This status of the key is pairing.
Paired	This status of the key is paired.
Terminating	This status of the key is terminating.

Key Track Receipt Status

Realized by implementation element:

Encoding values

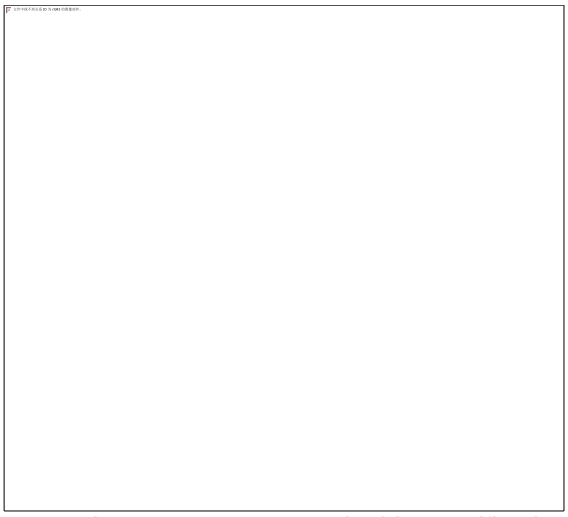
Enumeration Value	Enumeration Value Description
Valid	
Failure	
Awaiting Receipt	
Null	

KeyID

This is the unique identifier for the key being used.

Local Digital Key Record

Key record on the vehicle that contains information for Phone Digital Keys only (Not cards). Each record for a device that is CCC compliant (Phone) contains all of this information, along with the Local Pairing Record (as shown in image below). Local Pairing Record has information that is shared among Phone and Card pairing records.



Note: Please see Data Type in this specification for the most up to date information as this image may be out of date.

Properties of Value Types

Property	Property Description
KTS status	
Key Status	
Digital Key Type	
End Point PK	
Vehicle SK	
Vehicle PK	
Profile	
Date From	
Date To	
Slot ID	
cloudKTSFeedback	This flag signals confirmation that the a message has been successfully sent to the back-end signaling that a KTS receipt has been received by the vehicle. The flag defaults to false when a KTS is consumed by the NFC Controller. It is set to true when the Cloud confirms receipt of the NFC Cloud Event message.
Key Confirmed On Cloud	

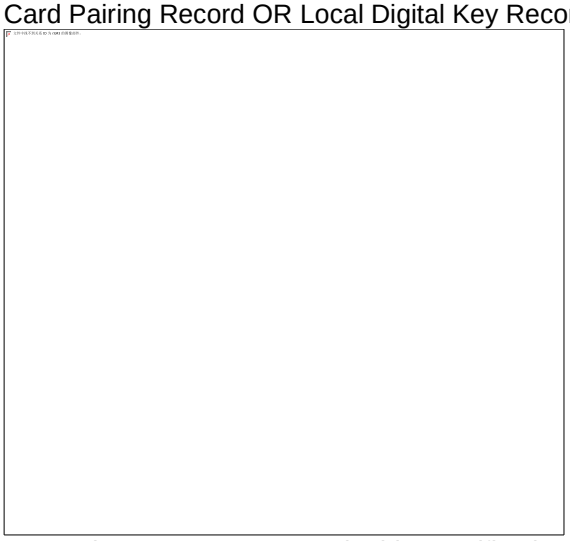
Local ID

The identifier generated by an NFC-enabled vehicle locally when an NFC command request is created using the onboard HMI.

This value is returned by the cloud backend system in traffic that corresponds to that particular command request, along with the cloud-generated Payload ID, in order to allow the vehicle to correlate the Local ID and Payload ID.

Local Pairing Record

This represents a pairing record on the NFC Controller. This record can either be for a NFC Card or Digital Key. As shown below, each record contains the data that is represented in Local Pairing Record, along with the data in Card Pairing Record OR Local Digital Key Record, depending on if it is a NFC Card or Digital Key.



Note: Please see Data Type in this specification for the most up to date information as this image may be out of date.

Properties of Value Types

Property	Property Description
Friendly Name	The unique name that is given to the key during initial pairing of a key that is on the pairing record local to the vehicle.
Key Type	The type of key on the pairing record local to the vehicle. This is the distinction between Factory/Retail/Fleet keys.
Pairing ID	The unique pairing identification number of a key on the pairing record local to the vehicle.
Key Index	The internal index of the NFC key, which is unique within all of the pairings stored in the module.
Device Type	

Local Pending Request Record

A Local Pending Request Record is saved whenever a retail user requests an NFC command using the in-vehicle HMI. It tracks the state of the request from the time it is made until the request is approved, denied, or times out.

When the NFC Cloud Backend replies to a request, either with an NFC Command Message or a denial notification, the Local Pending Request Record is deleted.

Properties of Value Types

Property	Property Description
Friendly Name	
Requested Command Type	
Request Timestamp	
Local ID	
Device Type	
Pairing ID	If the request is for pairing deletion, the Pairing ID of the pairing to be deleted.
FESN	

Locking Request

A request issued to the Body Control System's Power Locks Arbitrator, requesting a lock or unlock of the vehicle's doors. The exact behavior that this request triggers may vary based on the vehicle's configuration parameter and state.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Unlock	To indicate when a central unlock command is transmitted
Lock	To indicate when a central lock command is transmitted

Locking Requestor

Status of how the vehicle was previously locked

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Interior trim switch	Vehicle was locked using the interior trim switch
Else	Vehicle was locked not using the interior trim switch

Locking Source

The originator of a locking request.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
NFC Tap	Locked the vehicle using an exterior nfc reader
Interior Trim Switch	Locked the vehicle using the interior trim switch
Phone as a Key	Locked the vehicle from the exterior using a Phone as a key device
Keyfob	Locked from the exterior using a passive KeyFob
Door Cylinder	Locked from the exterior using a mechanical key

Module Data

Module specific DID, Configuration, and diagnostic specific data (as contained with part 2 spec)

Module Data Identifier

fixed 2 byte value for indicating a specific data identifier within the target system

Module Lock Status

Indicate whether a module is locked or unlocked, specific to Security Access (service 27h)

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description

Locked	Module is locked and the technician/service tool can only access read-only data
Unlocked	Module is unlocked and the technician/service tool can access read and write data

Module Unlock Key

12 fixed byte security key

MyKey Level

The active MyKey Level of a specific vehicle starting device while it is in use

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
MyKey	A vehicle was started with a device that has MyKey restrictions in place
Standard Key	A vehicle was started with a device that does not have MyKey restrictions in place
N/A	MyKey Level cannot be determined

NFC Cluster Message

The NFC feature-related messages that can be displayed in the vehicle's cluster.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Scan Digital Key To Drive	Cluster message prompting the user to scan an authorized NFC device in order to start or drive the vehicle
To Drive Press Brake And Start Button	Cluster message prompting the user to start the vehicle after they have scanned their NFC device
Null	No NFC feature-related indication requested.
Scan Digital Key And Press Brake To Shift Gear	Cluster message prompting the user to scan an NFC device in order to exit Secure Idle or Remote Start
Digital Key Programming Successful	Cluster message indicating that an attempt to pair an NFC device while in Factory Pairing Mode was successful
Digital Key Programming Fault	Cluster message indicating that an attempt to pair an NFC device while in Factory Pairing Mode has failed

NFC Command Type

The types of commands that can be issued by the NFC Cloud Backend System to the NFC System.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Add Key	Create a new pairing on a vehicle with the specified NFC key.
Delete Key	Remove a specific NFC key pairing.
Clear All Keys	Delete multiple/all User Keys
Restore Keys	Restore all factory and user keys (as part of module swap)

Request Key List	Transmit the list of paired and pending NFC keys to the cloud backend.
Cancel Request	The user has chosen to cancel a request before it was approved, denied, or timed out.

NFC Device Type

The device type is defined by the authentication protocol supported by the device. Ford NFC Cards are devices that support the Ford-specific NFC authentication protocol.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Ford NFC Card	A Ford provided NFC Card
CCC Smart Device	A smart device i.e. mobile phone or wearable

NFC Digita lKey Data

Determines if the data of digital keys paired is up to date.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Current	This is called when the key data on the Mobile App is current. The key data will turn to old after a set amount of time.
Old	This is called when key data on the Mobile App is old. If the user is requesting key data, it will need to request new data from the Cloud.

NFC Event Type

The NFC System's response to completing or attempting a specific device management, or configuration related request

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Key Pair - Success	The NFC System has received a key pairing command and executed it successfully. The key in question can now be used to access the vehicle.
Key Pair - Failure	The NFC System has received a key pairing command, but could not execute it successfully for some reason. The key in question may, but likely cannot, be used to access the vehicle.
Key Unpair - Success	The NFC System has received a key unpairing command and executed it successfully. The key in question can no longer be used to access the vehicle.
Key Unpair - Failure	The NFC System has received a key unpairing command but could not execute it successfully for some reason. The key in question can likely still be used to access the vehicle, but is not guaranteed to.
Enable Feature - Success	The NFC System received a command to enable the NFC feature behavior, and it was executed successfully.
Disable Feature - Failure	The NFC System received a command to disable the NFC feature behavior, but it could not be executed successfully for some reason. The NFC System is in an undefined state.

Enable Feature - Failure	The NFC System received a command to enable the NFC feature behavior, but it could not be executed successfully for some reason. The NFC System is in an undefined state.
Disable Feature - Success	The NFC System received a command to disable the NFC feature behavior, and it was executed successfully.
Master Reset - Success	The NFC System received a Master Reset signal locally on the vehicle, and successfully performed all of the appropriate actions in response (e.g., deleting keys).
Master Reset - Failure	The NFC System received a Master Reset signal locally on the vehicle, but one or more of the actions performed in response to the Master Reset event did not complete successfully. The NFC system is in an undefined state.
Modem Deauthorization - Success	The NFC System received a modem deauthorization event signal locally on the vehicle, and successfully performed all of the appropriate actions in response (e.g., deleting keys).
Modem Deauthorization - Failure	The NFC System received a modem deauthorization event signal locally on the vehicle, but one or more of the actions performed in response to the modem deauthorization event event did not complete successfully. The NFC system is in an undefined state.
Manufacturing Key Pairing - Success	The NFC System has successfully paired an NFC Device to the vehicle while it was in the "Factory programming allowed" state, during assembly.
Slot Inhibited - Succes	
Slot Inhibited - Failure	
Key Unpair - Key Started Success	

NFC Feature Package

Tells if the vehicle is equipped with the NFC feature.

NFC Key Type

The categories of keys that can exist in the NFC System.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Factory Key	NFC Card/device that was paired to the vehicle during assembly
Retail User Key	NFC Card/device that was programmed to the vehicle using the in-vehicle controls, (fleet management feature not active)
N/A	Key type cannot be determined
Fleet User Key	NFC Card/device that was remotely programmed to the vehicle while it was enrolled in the fleet management feature

NFC Location

The possible locations where an NFC tap event can occur.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Interior Reader	An NFC reader that can be accessed from the interior of the vehicle.
Exterior Reader	An NFC reader that can be accessed from the exterior of the vehicle with the doors locked.

NFC MyKey Creation Result

The possible outcomes of an NFC MyKey creation operation.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Successful	The MyKey creation was successful.
Unsuccessful - Already MyKey	The creation of the specified MyKey was unsuccessful because it is already configured as a MyKey.
Unsuccessful - Timeout waiting for tap	The driver did not take any additional actions for a set time (30 seconds by default) after initiating the MyKey creation process
Unsuccessful - Device not paired to vehicle	The device targeted for MyKey programming is not programmed to the vehicle

NFC Pairing Status

The possible states that an NFC card pairing can exist in on the Cloud Backend System.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Creation Requested	For a retail pairing, the pairing has been requested by a user from the in-vehicle HMI, but it has not yet been approved by the retail owner.
Creation Approved	The pairing is in the process of being transmitted to the vehicle and created onboard, but the vehicle has not yet confirmed that the pairing was created successfully. For retail pairings, this implies that the pairing was approved by the retail owner. This is the first state for pairings that are created through the FCS cloud backend or the service tool, because pairings created through these channels do not require approval. When a pairing is in this state, the associated NFC card may or may not be usable to unlock and start the vehicle.
Creation Command Delivered	
Creation Failed	An exception occurred during the creation or deletion of this pairing.
Active	The pairing has been transmitted to the vehicle, and the vehicle has confirmed that the pairing was created successfully. There is no deletion pending. The associated NFC card should be usable to open and start the vehicle.
Deletion Requested	For a retail card pairing, a retail user has requested deletion of this pairing through the in-vehicle HMI, but the retail owner has not yet approved the deletion request. Fleet and factory pairings never exist in this state, because they do not require approval. When a pairing is in this state, the associated NFC card should still be usable to unlock and start the vehicle.
Deletion Approved	
Deletion Command Delivered	The pairing, which was previously active on the vehicle, is in the process of being removed from the vehicle, but the vehicle has not yet confirmed that it successfully removed the pairing. The

	deletion command may or may not have been transmitted to the vehicle. For retail user pairings, this state implies that the retail owner has approved the deletion request. Fleet user pairings and factory pairings enter this state as soon as a deletion request is created, because changes to these types of pairings do not require approval. When a pairing is in this state, it may or may not be usable to unlock and start the vehicle.
Deletion Failed	

NFC Service Request Status

Indicate whether a NFC Service Request was accepted or rejected for failing a specific conditions(s)

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Accepted	Service request was accepted by the NFC Cloud
Rejected - Already a Factory Card	Service request to add Factory Card was rejected by the NFC Cloud because the selected device is already a Factory Card on the target vehicle
Rejected - Already a Retail User Card	Service request to add Retail User Card was rejected by the NFC Cloud because the selected device is already a Retail User Card on the target vehicle
Rejected - Already a Fleet User Card	Service request to add Fleet User Card was rejected by the NFC Cloud because the selected device is already a Fleet User Card on the target vehicle
Rejected - Not a Factory Card on vehicle	Service request to delete Factory Card was rejected by the NFC Cloud because the selected device isn't a Factory Card on the target vehicle
Rejected - Not a Retail Card on vehicle	Service request to delete Retail User Card was rejected by the NFC Cloud because the selected device isn't a Retail User Card on the target vehicle
Rejected - Not a Fleet Card on vehicle	Service request to delete Fleetl User Card was rejected by the NFC Cloud because the selected device isn't a Fleet User Card on the target vehicle
Rejected - No previous Factory Card pairings	Service request to restore Factory Cards was rejected by the NFC Cloud because the target vehicle had no previous Factory Cards to restore on the new/swapped module
Rejected - No previous Retail User Card pairings	Service request to restore Retail User Cards was rejected by the NFC Cloud because the target vehicle had no Retail User Cards to restore on the new/swapped module

NFC System Factory Pairing State

The states that the NFC system can exist in re: factory pairing behavior. When the NFC system is in Factory Pairing Mode, it will pair with any valid card presented, without backend authorization.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Factory Pairing Mode	The NFC System is in Factory pairing mode, where it can accept card pairings without requiring Ford Backend authorization

Normal Operation Mode	The NFC System is not in Factory pairing mode, and requires vehicle level and Ford Backend authorization in order to add or remove NFC Devices from the vehicle

NFC Tap Duration

The logical duration of a detected tap at one of the vehicle's NFC readers.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Short Tap	NFC Device was detected, authenticated, and kept within the readers range for less than 1 second
Long Tap	NFC Device was detected, authenticated, and kept within the readers range for 1-2.5 seconds

P2-UA_set

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
01 - door unlock	
02 - door lock	
03 - engine start first	
04 - engine start subsequent	

PIN

Identification number used to verify the key sharing session.

Pairing HMI Event

This determines how far the progress bar shall show to the user based on how far in the pairing process the system is.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Start	This is used when the user starts a pairing process is the vehicle.
Paired	This is used when the pairing process has been completed.
Awaiting KTS Receipt	This is used when pairing is still in progress, but the timeout has been reached and is waiting for the KTS still.
progress-10	This is used when progress of pairing has reached 10%.
progress-20	This is used when progress of pairing has reached 2 20%.
progress-30	This is used when progress of pairing has reached 30%.
progress-40	This is used when progress of pairing has reached 40%.
progress-50	This is used when progress of pairing has reached 50%.
progress-60	This is used when progress of pairing has reached 60%.
progress-70	This is used when progress of pairing has reached 70%.
progress-80	This is used when progress of pairing has reached 80%.

progress-90	This is used when progress of pairing has reached 90%.
Failed - System Failure	This is used when there has been a failure in the pairing process.
Failed - Vehicle Not In Pairing Mode	
Failed - Vehicle Safety Failure	
Failed - Pre-Conditions Not Met	

Pairing HMI Type

This will determine the type of pairing that is occurring to display to the user.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
NFC	This is used if the request comes in from an NFC Mobile device.
UWB	This is used if the request comes in from an UWB Mobile device.

Pairing ID

A unique identifier for a specific key pairing (digital key or NFC access card) on a vehicle. Pairing IDs are unique in context of a specific vehicle (i.e., two vehicles may have the same Pairing ID for different pairings, but the same Pairing ID can never be re-used on the same vehicle) and a specific pairing instance (i.e., if a pairing is deleted and recreated, the recreated pairing will have a new Pairing ID).

Pairing List Entry

Properties of Value Types

Property	Property Description
Key Index	
Key Type	
Device Type	
Friendly Name	
Card FESN	
Pairing ID	

Pairing Password

Password used for owner pairing that is defined by SPAKE protocol as defined by the CCC Specification.

Pairing Request Outcome

The possible outcomes

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
True	

True - Starting Key	
False	
Approved	The request was approved by the retail owner and the pairing was successfully created.
Denied	The request was denied by the retail owner, and the pairing has not been created.
Timed Out	The retail owner did not act on the request, and it has expired. The pairing has not been created.
Error	The retail owner approved the request, but there was a system error in the process of creating it. The pairing has not been created.

Pairing Response

The status of pairing response.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Pairing	This is used to tell the Cloud that the Verifiers were successfully saved on the vehicle.
Failed	This is used to tell the Cloud that the Verifiers failed to be saved on the vehicle.

Pairing Result

The result of the pairing event.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Paired	This is used when the result of CCC Phase 4 is paired and the device is ready to use.
Waiting Registration	This is used when the result of CCC Phase 4 is waiting registration.
Failed	This is used when the result of CCC Phase 4 is failed.
Pairing	This is used when the result of CCC Phase 4 is pairing.

Payload ID

The unique identifier assigned to a particular request by the cloud backend system.

Polling Result

The result of the Mobile App polling for the verifiers.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Timeout	This is used when the verifiers were not present within a certain time period.
Success	This is used when the verifiers have been successfully saved on the vehicle.

Public Certificate

800 Byte Public Key Certificate used as part of PKI process to verify whether a detected card is paired to the vehicle

Request ID

Unique identifier for a given request.

Retail Owner Approval Status

The possible states of a request for approval from a retail owner (such as a request to add a key).

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Pending	The retail owner has not taken an action on the request, and the request timeout has not expired.
Timed out	The request timeout expired without the retail owner taking any action.
Approved	The retail owner explicitly approved the request.
Denied	The retail owner explicitly denied the request.

Routine Data

Any specific data that needs to be included as part of initiating/completing a service tool initiated routine

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Nill	No additional data
Command Data	Encrypted payload received from the Cloud that needs to be delivered to the vehicle

Routine Id

Specific routine a service tool can request to run on the NFC System

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
701B - 00 Retail User Card Add Allowed	Request from Service tool to NFC System to verify if it can accept another Retail User Card
701B - 01 Fleet User Card Add Allowed	Request from Service tool to NFC System to verify if it can accept another Fleet User Card
701B - 02 Factory Card Add Allowed	Request from Service tool to NFC System to verify if it can accept another Factory Card
701B - 03 Retail User Card Delete Allowed	Request from Service tool to NFC System to verify if a selected NFC Card is present on the Module and is a Retail User Card

701B - 04 Fleet User Card Delete Allowed	Request from Service tool to NFC System to verify if a selected NFC Card is present on the Module and is a Fleet User Card
701B - 05 Factory Card Delete Allowed	Request from Service tool to NFC System to verify if a selected NFC Card is present on the Module and is a Factory Card
701B - 06 Clear All Cards Allowed	Request from Service tool to NFC System to verify if it active/communicating.
701B - 07 Restore Factory Cards Allowed	Request from Service tool to NFC System to verify if it is a new/swapped module with no Factory Cards currently present on the system
701B - 08 Restore Retail User Cards Allowed	Request from Service tool to NFC System to verify if it is a new/swapped module with no Retail User Cards currently present on the system
701A - 01 Deliver NFC Command Payload	Used to inject encrypted (SyncP) payload received from cloud into the vehicle

Routine Result

Response sent from the vehicle system to the service tool after receiving a command or data from it

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
701B - Pass	Routine completed successfully, no additional data
701B - Fail	Routine did not complete successfully, no additional data
701A - NFC Cloud Event Payload	Routine completed successfully, additional payload that needs to be received by service tool and delivered to cloud

Secure Idle Status

The state of the vehicle's Secure Idle feature.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Secure Idle Active	The vehicle is locked in secure idle - cannot shift out of park while vehicle is running
Secure Idle Inactive	The vehicle has exited secure idle - vehicle can shift out of Park while vehicle is running
Secure Idle Unknown	State of secure idle cannot be determined

Server Remote Termination Request

A termination request that is sent remotely to the server.

Session ID

Unique identifier for each session.

Sharing Session

Data needed to determine the sharing session as defined by Section 17 in the CCC Specification.

Sharing Session Record

Record of all sharing sessions on the vehicle.

Starting Authorization Source

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Digital Key	A Ford NFC access card, or a CCC-compatible digital key stored on a smart device.
PaaK Gen1	A Phone-as-a-Key device that is not compatible with the CCC Digital Key standard.
Key Fob/IKT	A passive-start vehicle keyfob.
null	A bladed key with an in-key transponder.

Termination Event

The different event types related to termination.

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
dRTR	Delete Remote Termination Request - This is used when a key is remotely terminated.
tA	Termination Attestation - Used when a termination is request by someone who is not the key being deleted. Ex: Owner deletes friend key.
no_tA	This is sued when to attestation is present. This is used for a case like security breach where no attestation is required.
mobileReq	This is used when the termination request has come from a mobile device.
vehicleReq	This is used when the termination request has come from the vehicle.
exp	This is used when a friend key expires.
vehicle_tA	This is used when the attestation comes from the vehicle. Used in In-Vehicle termination of keys.
chgOwner	This is used when there has been a request to change the owner device
reset	This is used when a reset on the device has been requested.
dAuth	This is called when th vehicle has been deauthorized.

Timestamp

A date and time specification in RFC 3339 "date-time" format, for example 1985-04-12T23:20:50.52Z.

Transaction Result

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
success	
failed	

UID

The Unique Identifier of an NFC device, as defined in ISO 14443.3.

VIN

A Vehicle Identification Number in 17-character FMVSS 115 or ISO 3779 format.

Vehicle Line

Realized by implementation element:

Vehicle Verifiers Status

Status of verifier on vehicle.

Verifiers

Used for owner pairing on the vehicle that is defined by the CCC Specification.

Properties of Value Types

Property	Property Description
w0	
L	
salt	

friendlyName

result

Realized by implementation element:

Encoding values

Enumeration Value	Enumeration Value Description
Unsupported	This is used if the status of the manageKey API received back from the Native App was determined to be unsupported.
Valid	This is used if the status of the manageKey API received back from the Native App was determined to be valid.
Invalid	This is used if the status of the manageKey API received back from the Native App was determined to be invalid.

6.1.4 Technical Signals

6.1.4.1 GSDB Signals

AdminMyKeyTot_No_Actl

Signal Name	AdminMyKeyTot_No_Actl
Description	Provides indication status of how many admin keys exist
Encoding	UnitlessValue8bit_ET
Transmitter	BCM
Receiver	APIM
Logical Signal	NFC MyKey - Creation Status

DgtlKeyType_D_Stat

Signal Name	DgtlKeyType_D_Stat
Description	
Encoding	ActivePassiveNull_ET
Transmitter	NFAM ECG
Receiver	ECG BCM
Logical Signal	

Ext1_AID

Signal Name	Ext1_AID
Description	Indicates the AID that is present and selected on the NFC device (9 bytes in length)
Encoding	UnitlessValue9Bytes_ET
Transmitter	NFC Reader
Receiver	NFAM
Logical Signal	Device Type

Ext1_APDU_CLA

Signal Name	Ext1_APDU_CLA
Description	Instruction class - indicates the type of command, e.g. interindustry or proprietary. Part of Command APDU sent from Reader to Device
Encoding	UnitlessValue8bit_ET
Transmitter	NFAM
Receiver	NFC Reader
Logical Signal	

Ext1_APDU_Data

Signal Name	Ext1_APDU_Data
Description	The actual command data sent over APDU as part of the command

Encoding	UnitlessValue255bit_ET
Transmitter	NFAM
Receiver	NFC Reader
Logical Signal	

Ext1_APDU_INS

Signal Name	**Ext1_APDU_INS**
Description	Instruction code - indicates the specific command, e.g. "write data". Part of Command APDU sent from Reader to Device
Encoding	UnitlessValue8bit_ET
Transmitter	NFAM
Receiver	NFC Reader
Logical Signal	

Ext1_APDU_Len

Signal Name	**Ext1_APDU_Len**
Description	Indicates length of command data to follow as part of Command APDU sent from Reader to Device
Encoding	UnitlessValue8bit_ET
Transmitter	NFAM
Receiver	NFC Reader
Logical Signal	

Ext1_APDU_Param

Signal Name	**Ext1_APDU_Param**
Description	Instruction parameters for the command, e.g. offset into file at which to write the data. Part of Command APDU sent from Reader to Device
Encoding	UnitlessValue16bit_ET
Transmitter	NFAM
Receiver	NFC Reader
Logical Signal	

Ext1_APDU_RspLen

Signal Name	**Ext1_APDU_RspLen**
Description	Indicated length of response data to expect from Device as part of Reponse APDU
Encoding	UnitlessValue8bit_ET
Transmitter	NFAM
Receiver	NFC Reader
Logical Signal	

Ext1_APDU_Rsp_Data

Signal Name	Ext1_APDU_Rsp_Data
Description	Data received from Device as part of Response APDU
Encoding	UnitlessValue255bit_ET
Transmitter	NFC Reader
Receiver	NFAM
Logical Signal	

Ext1_APDU_StatByte

Signal Name	Ext1_APDU_StatByte
Description	Command processing status provided back from device as part of Response APDU
Encoding	UnitlessValue16bit_ET
Transmitter	NFC Reader
Receiver	NFAM
Logical Signal	

Ext1_Card_Infield_D_Stat

Signal Name	Ext1_Card_Infield_D_Stat
Description	Indicated whether an NFC Device is within or has exited the detection range of an NFC Reader
Encoding	Ext1_Card_Infield_D_Stat_ET
Transmitter	NFC Reader
Receiver	NFAM
Logical Signal	NFC Device Detected Device Exited Field Device Entered Field Location

Ext1_FaultStatus

Signal Name	Ext1_FaultStatus
Description	Indicates whether there is an active fault at the reader or during communication with the device
Encoding	Ext1_FaultStatus_ET
Transmitter	NFC Reader
Receiver	NFAM
Logical Signal	

Ext1_UID_Data

Signal Name	Ext1_UID_Data
Description	Indicated the NFC Devices Unique Identifier
Encoding	UnitlessValue256bit_ET
Transmitter	NFC Reader

Receiver	NFAM
Logical Signal	

FactoryReset_Rq

Signal Name	**FactoryReset_Rq**
Description	Request to reset back to factory defaults
Encoding	ModemResetDRq_ET
Transmitter	
Receiver	NFAM
Logical Signal	Master Reset Command

Ignition_Status

Signal Name	**Ignition_Status**
Description	Ignition status of the vehicle
Encoding	Ignition_Status_ET
Transmitter	
Receiver	
Logical Signal	Start Button Press

ImmoMsgTxt_D_Rq

Signal Name	**ImmoMsgTxt_D_Rq**
Description	Provides a trigger indication to IPC after BCM system performs key search
Encoding	immoMsgTxt_D_Rq_ET
Transmitter	BCM
Receiver	IPC
Logical Signal	Key Search Request Indication Vehicle Cluster Message

KeyMykeysTot_No_Actl

Signal Name	**KeyMykeysTot_No_Actl**
Description	Provides indication of total count for how many mykeys exist
Encoding	UnitlessValue8bit_ET
Transmitter	BCM
Receiver	APIM
Logical Signal	NFC MyKey - Creation Status

LifeCycMde_D_Actl

Signal Name	**LifeCycMde_D_Actl**

Description	Indicates the status of the vehicle mode (Factory, Transport, Normal)
Encoding	LifeCycMdeDActl_ET
Transmitter	
Receiver	
Logical Signal	Manufacturing Pairing Event

LocationServices_3

Signal Name	**LocationServices_3**
Description	Provides network time from GNSS to vehicle
Encoding	Unitless64bit_ET
Transmitter	
Receiver	
Logical Signal	

ModemAuthrz_D_Stat

Signal Name	**ModemAuthrz_D_Stat**
Description	Provides modem authorization status
Encoding	ModemAuthrzDStat_ET
Transmitter	
Receiver	
Logical Signal	Modem Deauthorization

ModemReset_D_Rq

Signal Name	**ModemReset_D_Rq**
Description	Instructs specific components to perform a reset
Encoding	ModemResetDRq_ET
Transmitter	
Receiver	
Logical Signal	Modem Deauthorization

NFC_Enable_Status

Signal Name	**NFC_Enable_Status**
Description	Whether the NFC Feature is "Enabled" or "Disabled" on the NFC System
Encoding	DisableEnable_ET
Transmitter	
Receiver	
Logical Signal	

NFC_FaultDisable_Status

Signal Name	NFC_FaultDisable_Status
Description	If a fault has caused the NFC System to "Disable" the NFC feature on the NFC System
Encoding	DisableEnable_ET
Transmitter	
Receiver	
Logical Signal	

NFC_Polling_Freq

Signal Name	NFC_Polling_Freq
Description	Frequency of polling. 10Hz by default
Encoding	frequency[hertz]
Transmitter	
Receiver	
Logical Signal	

NfcDevcAuthrzT_B_Rq

Signal Name	NfcDevcAuthrzT_B_Rq
Description	This signal is responsible for sending a request to cancel authorization when exterior lock status = lock
Encoding	NullValid_ET
Transmitter	BCM ECG
Receiver	NFAM ECG
Logical Signal	Trigger Deauthorization

NfcDevcAuthrz_T_Actl

Signal Name	NfcDevcAuthrz_T_Actl
Description	Provides the seconds of time left in the authorization window.
Encoding	UnitlessValue8bit_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Time Remaining Starting Authorized Status Indication

NfcDevcCmd_No_Actl

Signal Name	NfcDevcCmd_No_Actl
Description	The key index of the key related to this event, if any
Encoding	UnitlessValue8bit_ET

Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Key Index

NfcDevcDetct_D_Stat

Signal Name	**NfcDevcDetct_D_Stat**
Description	Indicates the location of the detected device
Encoding	NFCDevcDetct_D_Stat
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Location

NfcDevcKeyType_D_Stat

Signal Name	**NfcDevcKeyType_D_Stat**
Description	Provides Indication for the type of the Near Field Communication (NFC) device - Factory or User.
Encoding	UserFactoryNull_D_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Key Search Response Authorizing key type

NfcDevcPair_D_Stat

Signal Name	**NfcDevcPair_D_Stat**
Description	Provides indication when a device is paired so vehicle can blink the lights, lock/unlock doors, display cluster popups.
Encoding	SuccessFailNull_D_ET
Transmitter	ECG NFAM
Receiver	BCM ECG
Logical Signal	Successful Manufacturing Pairing Event

NfcDevcSearchId_No_Actl

Signal Name	**NfcDevcSearchId_No_Actl**
Description	The Near Field Communication (NFC) key index of the key that is authorizing vehicle start, if starting is authorized.

Encoding	UnitlessValue8bit_ET
Transmitter	NFAM ECG
Receiver	ECG BCM
Logical Signal	Authorizing key Key Search Response

NfcDevcSearch_B_Rq

Signal Name	**NfcDevcSearch_B_Rq**
Description	Key Search request from the vehicle control function
Encoding	ActiveInactive_ET
Transmitter	ECG BCM NFAM
Receiver	NFAM ECG
Logical Signal	Key Search Request

NfcDevcSearch_B_Stat

Signal Name	**NfcDevcSearch_B_Stat**
Description	Search request result
Encoding	ValidInvalidNull_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Key Search Response Authorized

NfcDevcSearch_No_Rq

Signal Name	**NfcDevcSearch_No_Rq**
Description	Signal that includes rolling count transmitted by the Body Control Module (BCM) and used to synchronize specific signals with corresponding specific event.
Encoding	UnitlessValue3bit_ET
Transmitter	BCM ECG
Receiver	ECG NFAM
Logical Signal	Key Search Request

NfcDevcSrch1_No_Actl

Signal Name	**NfcDevcSrch1_No_Actl**

Description	Signal that includes rolling count transmitted by the Near Field Authorization Module (NFAM) and used to align a search request with the corresponding search result, synchronized with NfcDevcSrch2_No_Actl
Encoding	UnitlessValue3bit_ET
Transmitter	NFAM
Receiver	ECG BCM
Logical Signal	Authorizing key Key Search Response

NfcDevcSrch2_No_Actl

Signal Name	**NfcDevcSrch2_No_Actl**
Description	Signal that includes rolling count transmitted by the Near Field Authorization Module (NFAM) and used to align a search request with the corresponding search result, synchronized with NfcDevcSrch1_No_Actl
Encoding	UnitlessValue3bit_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Key Search Response Authorized

NfcDevcTap1_No_Rq

Signal Name	**NfcDevcTap1_No_Rq**
Description	Event counter transmitted during "tap" event, synchronized with NfcDevcTap2_No_Rq
Encoding	UnitlessValue3bit_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	NFC Tap Message

NfcDevcTap2_No_Rq

Signal Name	**NfcDevcTap2_No_Rq**
Description	Event counter transmitted during "tap" event, synchronized with NfcDevcTap_No_Rq_QM
Encoding	UnitlessValue3bit_ET
Transmitter	NFAM ECG
Receiver	ECG BCM
Logical Signal	NFC Tap Message

NfcDevcTapDur_D_Stat

Signal Name	NfcDevcTapDur_D_Stat
Description	Provides Indication for the Tap duration, short or long; used by the Body Control Module (BCM) logic to understand what action to take.
Encoding	LongShortNull_D_ET
Transmitter	NFAM ECG
Receiver	ECG BCM
Logical Signal	Tap Duration

NfcDevcTapId_No_Actl

Signal Name	NfcDevcTapId_No_Actl
Description	Indicates keyindex of 1 of up to 255 Near Field Communication (NFC) enabled devices and corresponds to the device found.
Encoding	UnitlessValue8bit_ET
Transmitter	ECG NFAM
Receiver	BCM ECG
Logical Signal	Key Index NFC Tap Message

NfcDevcTapMsg_No_Cnt

Signal Name	NfcDevcTapMsg_No_Cnt
Description	Counter for dependability evaluation of NfcTapMessage_ASIL message.
Encoding	UnitlessValue4bit_ET
Transmitter	NFAM ECG
Receiver	ECG BCM NFAM
Logical Signal	Paired NFC Tap Message

NfcDevcTapMsg_No_Crc

Signal Name	NfcDevcTapMsg_No_Crc
Description	Cyclic Redundancy Check (CRC) for dependability evaluation of NfcTapMessage_ASIL messagel.
Encoding	UnitlessValue8bit_ET
Transmitter	NFAM ECG
Receiver	BCM ECG NFAM
Logical Signal	Paired

	NFC Tap Message

NfcDevcTapPrd_B_Stat

Signal Name	NfcDevcTapPrd_B_Stat
Description	Provides Indication when the Tap Event is authorized or not authorized
Encoding	YesNo_ET
Transmitter	NFAM ECG
Receiver	ECG BCM
Logical Signal	Paired NFC Tap Message

NfcDevc_D_Cmd

Signal Name	NfcDevc_D_Cmd
Description	Indicates what kind of command was requested
Encoding	NfcDevcCmd_D_Rq_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Command Type

NfcDevc_D_Dsply

Signal Name	NfcDevc_D_Dsply
Description	This signal is transmitted by Body Control Module (BCM) as a result of key search to trigger Near Field Communication (NFC) related warnings in cluster.
Encoding	NfcDevcDsply_D_Rq_ET
Transmitter	BCM
Receiver	IPC
Logical Signal	NFC Cluster Message Indication

NfcDevc_D_Stat

Signal Name	NfcDevc_D_Stat
Description	Indicates the status of Near Field Communication (NFC) Command.
Encoding	SuccessFailNull_D_ET
Transmitter	ECG NFAM
Receiver	BCM ECG
Logical Signal	Outcome

NfcMyKeyCreate_D_Rq

Signal Name	NfcMyKeyCreate_D_Rq
Description	A request to create a new MyKey from an NFC device
Encoding	RequestNull_ET
Transmitter	APIM
Receiver	BCM
Logical Signal	NFC MyKey - Wait for New MyKey

NfcMyKeyCreate_D_Stat

Signal Name	NfcMyKeyCreate_D_Stat
Description	Provides indication status when mykey has been created
Encoding	NfcMyKeyCreate_D_Stat_ET
Transmitter	BCM
Receiver	APIM
Logical Signal	NFC MyKey - Creation Status NFC MyKey Creation Status NFC MyKey - Ready For New MyKey NFC MyKey Creation Result

NfcSerial_D_Rq

Signal Name	NfcSerial_D_Rq
Description	Signal used to as part of initiating NFAM module provisioning process
Encoding	NFCProvDID_ET
Transmitter	ECG
Receiver	NFAM
Logical Signal	

NfcSrchRespMsg_No_Cnt

Signal Name	NfcSrchRespMsg_No_Cnt
Description	Counter for dependability evaluation of NfcKeySearchMessage message.
Encoding	UnitlessValue4bit_ET
Transmitter	ECG BCM
Receiver	ECG NFAM
Logical Signal	Key Search Request

NfcSrchRespMsg_No_Crc

Signal Name	NfcSrchRespMsg_No_Crc
Description	Cyclic Redundancy Check (CRC) for dependability evaluation of NfcKeySearchMessage message.

Encoding	UnitlessValue8bit_ET
Transmitter	ECG BCM
Receiver	ECG NFAM
Logical Signal	Key Search Request

NfcSrchRqMsg_No_Cnt

Signal Name	**NfcSrchRqMsg_No_Cnt**
Description	Counter for dependability evaluation of NfcDevcSearch_B_Stat signal.
Encoding	UnitlessValue4bit_ET
Transmitter	ECG NFAM
Receiver	BCM ECG
Logical Signal	Authorized Key Search Response

NfcSrchRqMsg_No_Crc

Signal Name	**NfcSrchRqMsg_No_Crc**
Description	Cyclic Redundancy Check (CRC) for dependability evaluation of NfcDevcSearch_B_Stat signal.
Encoding	UnitlessValue8bit_ET
Transmitter	ECG NFAM
Receiver	ECG BCM
Logical Signal	Authorized Key Search Response

PwPckTq_D_Stat

Signal Name	**PwPckTq_D_Stat**
Description	Provides indication if the vehicle is in motive or non-motive mode: PwPckTq_D_Stat = 0x0 (PwPckOff_TqNotAvailable) e.g. engine is not running PwPckTq_D_Stat = 0x1 (PwPckOn_TqNotAvailable) e.g. engine is running in NonMotive mode PwPckTq_D_Stat = 0x2 (StartInprgrss_TqNotAvail) e.g. engine is cranking PwPckTq_D_Stat = 0x3 (PwPckOn_TqAvailable) e.g. engine is running in Motive mode
Encoding	PwPckTqDStat_ET
Transmitter	ECG
Receiver	NFAM
Logical Signal	Ignition Status

Remote_Start_Status

Signal Name	Remote_Start_Status
Description	Provides indication if vehicle is in Remote start mode
Encoding	RemoteStartStatus_ET
Transmitter	
Receiver	
Logical Signal	Remote Start Status Remote Start Status

VehStrtKeyIndx_No_Actl

Signal Name	VehStrtKeyIndx_No_Actl
Description	
Encoding	UnitlessValue8bit_ET
Transmitter	
Receiver	
Logical Signal	

VehStrtKeySrc_D_Stat

Signal Name	VehStrtKeySrc_D_Stat
Description	
Encoding	VehStrtKeySrc_D_Stat_ET
Transmitter	
Receiver	
Logical Signal	

VehStrtKeyType_D_Stat

Signal Name	VehStrtKeyType_D_Stat
Description	
Encoding	UserFactoryNull_D_ET
Transmitter	
Receiver	
Logical Signal	

Veh_Lock_Status

Signal Name	Veh_Lock_Status
Description	Provides indication of vehicle lock status
Encoding	Veh_Lock_Status_ET
Transmitter	
Receiver	
Logical Signal	

6.1.5 Technical Parameters

NfcControllerResponseTimeout

Name	NfcControllerResponseTimeout
Description	
Encoding Type	
ECU	APIM

6.2 Glossary

6.2.1 Definitions

Definition	Description
Pairing	A pairing is a relationship between a specific NFC device and a specific vehicle. When an NFC device and a vehicle are paired, the NFC device can generally be used to unlock and start the vehicle, although it may be possible to limit specific permissions (e.g., trunk unlocking) granted to a particular NFC device.
Retail admin	TODO define

Table 6: Definitions used in this document

6.2.2 Abbreviations

No acronyms specified.

Document ends here.