Function (Group) Specification

Function Group Spec

F002070-Near_Field_Communication-abonnel1

Custom Scope

Document Type	**Function Specification**	
Template Version	**6.0**	
SysML Report Template Version	**M (4/16/2019)**	
Document ID	**2021-08-06 nfc entry and starting - driver information system function specification - p702mca application.docx**	
Document Location		
Document Owner	**MyName**	
Document Revision	**FGS0**	
Document Status	**Draft**	
Date Issued	**2021-08-06**	
Date Revised	**2021-08-06**	
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.

$

List of Figures

List of Tables

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

Name	CDSID	Org.	Title	Project Role
John Van Wiemeersch	jvanviem	RA&E, Adv. Feat. Development	Supervisor	Design Support
Aaron DeLong	adelong2	RA&E, Adv. Feat. Development	Research Engineer	Research Design Lead
Vivek Elangovan	velango5	RA&E, Adv. Feat. Development	Research Engineer	Design Support
Rita Trupiano	mtrupia1	PD, Sys. Eng., Distributed Feat.	Feature Owner Supervisor	Feature Owner Supervisor
Eugene Karpinsky	ekarpins	PD, Sys. Eng., Distributed Feat.	Core Feature Owner	Production Design Lead and Feature Owner
Farhan Ehsan	fehsan2	PD, Sys. Eng., Distributed Feat.	Core Feature Owner	Production Design Lead and Feature Owner
Aaron Bonnell-Kangas	abonnel1	PD, Sys. Eng., Distributed Feat.	Core Feature Owner	Production Design Lead and Feature Owner
Jonathon Wolf	jwolf53	PD, Sys. Eng., Distributed Feat.	Core Feature Owner	Production Design Lead and Feature Owner
Matt Swis	mswis	PD, EESE, Body & Security Elec.	Core Security & RF Supervisor	NFC System Owner Supervisor
Nisha Patel	npate152	PD, EESE, Body & Security Elec.	Core NFC Engineer	NFC System Owner
David Hernandez	dhern138	PD, EESE, Body & Security Elec.	Core NFC Engineer	NFC System Owner
Suthagaran Nagarasa	snagaras	PD, EESE, Body & Security Elec.	Core NFC Engineer	NFC System Owner
Kevin Hille	khille	PD, EESE, Body & DAT SW	Technical Specialist – Immob.	NFC Immobilizer Function Owner, Design Support
John Ricks	jricks7	PD, EESE, Body & DAT SW	Software Supervisor	Software Supervisor
John Popovecz	jpopovec	PD, EESE, Body & DAT SW	Body Module SW Supervisor	Body Module SW Supervisor
Hosam Irsheid	hirsheid	PD, EESE, Body & DAT SW	Software Engineer	Software Design
Sam Mehdi	hmehdi	PD, EESE, Body & DAT SW	Product Design Engineer	Software Design
Vishala Pasala	vpasala	PD, EESE, Body & DAT SW	Software Engineer	Software Design
Maeen Mawari	mmawari	PD, EESE, Body & DAT SW	MBSE Engineer	Software Design

Eric Reed	ereed2	PD, EESE, Body & DAT SW	VSC SW Engineer	Software Design
Ahmad Sabri	asabri3	PD, EESE, Body & DAT SW	PD Engineer	Software Design
Jeff Lossing	jlossing	PD, EESE, Body & DAT SW	Software Engineer	Software Design
Andrew Hall	ahall185	PD, EESE, Body & DAT SW	Design Engineer, BCM Software	Software Design
Sachin Magar	smagar	PD, EESE, Body & DAT SW	Design Engineer, BCM Software	Software Design
Akshita Kulkarni	akulka2	PD, EESE, Body & DAT SW	Design Engineer, BCM Software	Software Design
Adithya Ramachandran	aramac11	PD, EESE, Body & DAT SW	Software Engineer	Software Design
S Bagga	sbagga11	PD, EESE, Body & DAT SW	Software Engineer	Software Design
Gail Cheng	gcheng	PD, In-Vehicle Infotainment & Connectivity	Infotainment Systems Supervisor	Infotainment System Design Supervisor
Matthew Borrelli	mborrel4	PD, In-Vehicle Infotainment & Connectivity	Infotainment Systems Engineer	Infotainment System Design
Laura Check	lburek	PD, In-Vehicle Infotainment & Connectivity	SYNC Supervisor	SYNC System Supervisor
Iqbal Faheem Sayyed	isayyed	PD, In-Vehicle Infotainment & Connectivity	SYNC Technical Program Manager	SYNC Technical Program Manager
Scott Watkins	swatkins	PD, In-Vehicle Infotainment & Connectivity	DI Technical Expert	Driver Information Design Support
Stavros Dionyssopoulos	sdionyss	PD, CIED	DI HMI Engineer	Driver Information HMI Support
Nicholas Davio	ndavio	PD, CIED	HMI Supervisor	HMI Support Supervisor
Mack Dobbie	mdobbie	PD, CIED	HMI Designer	HMI Support
Montana Pruett	mpruett2	PD, CIED	I&E Engineer	I&E Support
Patrick Brautigan	pbrautig	PD, CIED	UX Engineer	UX Support
Jeffrey Hamel	jhamel7	PD, Enterprise Connectivity	Product Owner, TPM	Ford Mobile App Design
Michael Martinez	mmart6664	PD, Mobility	Product Manager	Ford Mobile App Design
Bruce Williams	bwilli28	PD, EESE, Netcom Core	Product Design Engineer	Electrical Architecture Consult
Jim Lawlis	jlawlis	PD, EESE, Advanced Netcom	Technical Specialist - Netcom	Electrical Architecture Consult
Nhi Torres	ntorres5	PD, EESE, Netcom Diag.	Supervisor	Electrical Architecture Consult
Eric Paton	epaton	PD, EESE, Netcom Diag.	Engineer	Electrical Architecture Consult
Ankita Vyas	avyas8	PD, EESE, Functional Safety	Functional Safety Engineer	Functional Safety Consult
Ahmet Cinar	acinar1	PD Europe, Underbody EESE	Tech. Expert – Closure Electronics	Closure Design Consult

					1.3
Uwe Zank	uzank	PD Europe, Underbody EESE	Supervisor, Security Electronics	Security Design Consult	
Denney Vellaramkalayil	dvellara	PD Europe, Underbody EESE	System Engineer, Locking Application	Locking Design Support	
Henry Popow	hpopow	Quality, EESE	Quality Engineer	Quality Coach	
Gerard Szczepaniak	gszczepa	Quality, EESE	Quality Engineer	Quality Coach	
Christina Bloxsom	cbloxsom	SE&SE, ASO, Adv. Policy	Subject Matter Expert	Safety & Regulations Consult	
Mike Westra	mwestra	IT, Cybersecurity	Technical Leader – Security	Cybersecurity Consult	
Jochen Schubert	jschub1	IT, Cybersecurity	Cybersecurity Engineer	Cybersecurity Design Support	
Dan Zajac	dzajac8	IT, Cybersecurity	Cybersecurity Supervisor	Cybersecurity Supervisor	
Jacob Nelson	jnels148	IT, Cybersecurity	Cybersecurity Engineer	Cybersecurity Design Support	
Xin Ye	xye7	IT, Cybersecurity	Technical Specialist - Security	Cybersecurity Consult	
Simon Hurr	shurr	IT, Cybersecurity	Security Application Specialist	Cybersecurity Consult	
Mike Simons	msimon78	IT, CVP&P, PaaK	Systems Engineer	Off Board Function Owner Lead	
Faten Fawaz	ffawaz	IT, CVP&P, Basic Design	Basic Design Architect	Backend Infrastructure Design Lead	
Steve Craig	scraig33	IT, CVP&P, Integration	Technical Program Manager	Backend Infrastructure Design Support	
Yona Shaposhnik	yshaposh	IT, MPS, Mobility Arch.	Solution Architect	Backend Infrastructure Design Support	
Michelle Moody	mmoody1	IT, Mobility, FCS	Director	Project Champion – Fleet	
Robert Johnson	rjohns75	IT, Mobility, FCS	Product Marketing Manager	Project Champion – Fleet	
Mustapha Elkhatib	melkhat1	IT, Mobility, FCS	Product Manager	Fleet Infrastructure Design Support	
Geoffrey Scofield	gscofiel	IT, Mobility, FCS	Product Engineer	Fleet Infrastructure Design Support	
Jennifer Oak	joak	MS&S, US Marketing	Connected Marketing Manager	Project Champion – Retail	
Timothy Son Hing	tsonhin1	MS&S, US Marketing	Marketing Manager	Project Champion – Retail	

Document Conventions

1.3.1 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*.

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

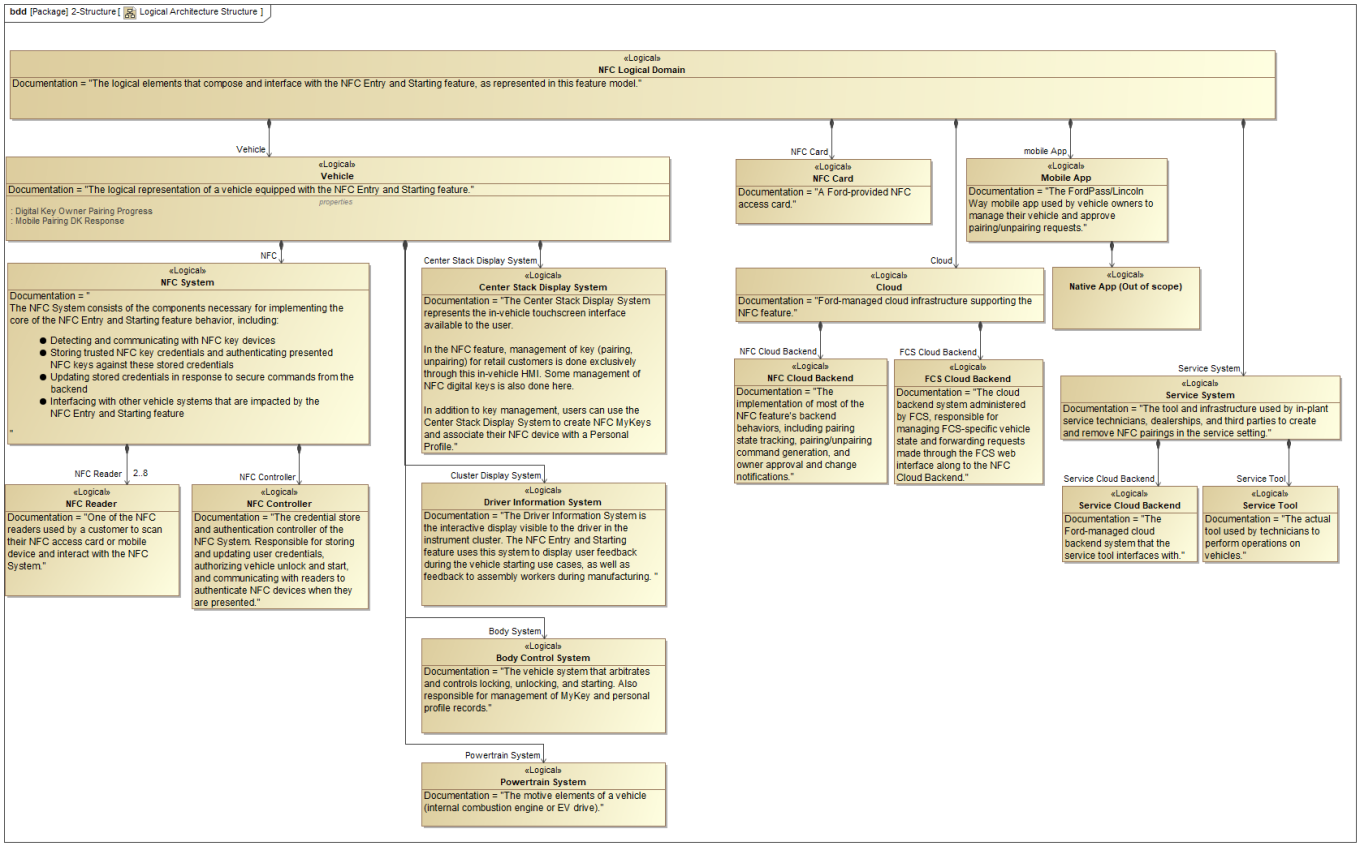


Figure 1: NFC Logical Domain Structure

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.

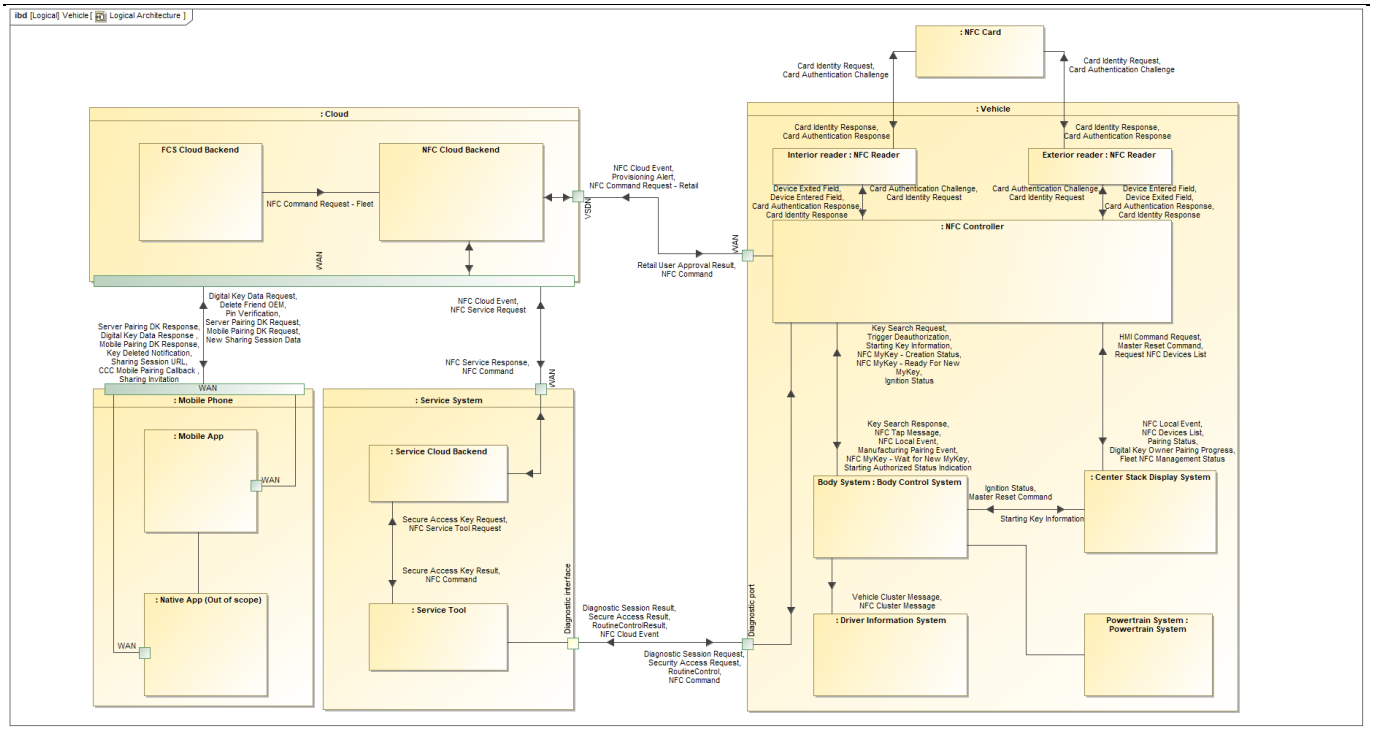


Figure 2: NFC Logical Architecture

3 FUNCTION GROUP DESCRIPTION

This specification consists of documentation about the logical system component **Driver Information System.**.

The Driver Information System is the interactive display visible to the driver in the instrument cluster. The NFC Entry and Starting feature uses this system to display user feedback during the vehicle starting use cases, as well as feedback to assembly workers during manufacturing.

3.1 Logical System Behavior

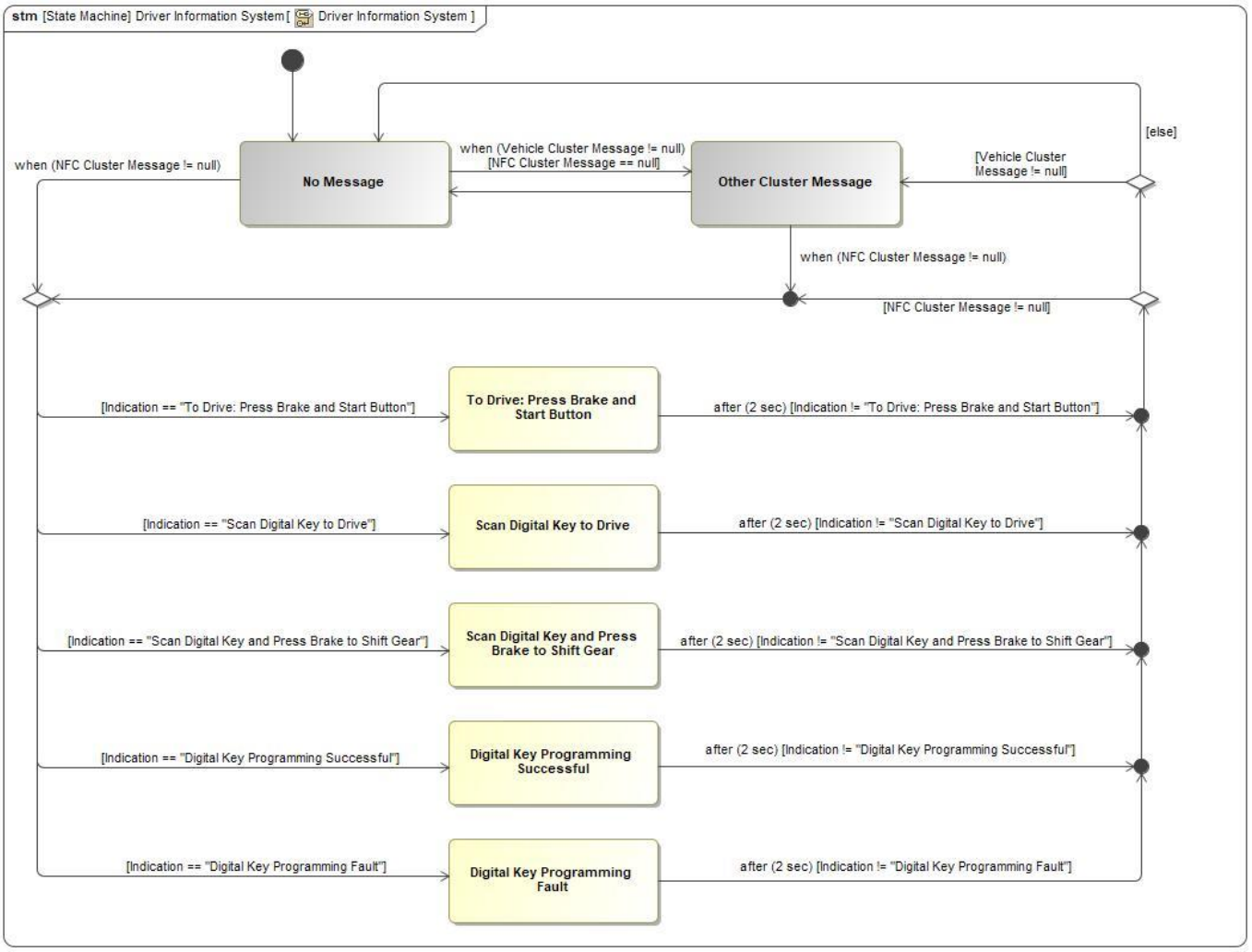


Figure 3: Driver Information System

3.1.1 Driver Information System Screens

State	Description	Requirements Reference
Digital Key Programming Fault	Displayed during vehicle manufacturing, if a technician attempts	SR Driver Information System: message availability in Limited mode

	to pair another NFC card with the vehicle but an error occurs.	Driver Information System: "Digital Key Programming Fault" message details Driver Information System: message display logic
Digital Key Programming Successful	Displayed during vehicle manufacturing, if a technician successfully creates an NFC card pairing.	Driver Information System: message availability in Limited mode Driver Information System: "Digital Key Programming Successful" message details Driver Information System: message display logic
No Message		Driver Information System: display time for "To Drive: Press Brake and Start Button" and "Scan Digital Key To Drive" Driver Information System: display time for "Scan Digital Key And Press Brake to Shift Gear" message
Other Cluster Message	Any of the other cluster messages not related to this feature that can be displayed to the driver.	
Scan Digital Key and Press Brake to Shift Gear	Displayed in certain cases when the NFC system is not in the “starting authorized” state, to prompt the user in exiting Secure Idle	Driver Information System: "Scan Digital Key And Press Brake To Shift Gear" message details Driver Information System: message display logic
Scan Digital Key to Drive	Displayed in certain cases when the NFC system is not in the “starting authorized” state, to prompt the user to authorize starting	Driver Information System: message availability in Limited mode Driver Information System: "Scan Digital Key To Drive" message details Driver Information System: message display logic
To Drive: Press Brake and Start Button	Displayed on non-DCO vehicles in certain cases when the NFC system is in the “starting authorized” state, to prompt the user to begin driving.	Driver Information System: message availability in Limited mode Driver Information System: "To Drive: Press Brake And Start" message details Driver Information System: message display logic

Table 1: Operation Modes and States on Driver Information System

3.1.2 Driver Information System requirements

REQ-NFC-ES-311 Driver Information System: message display logic

The Driver Information System shall display warnings based on the "Indication" signal of the "NFC Cluster Message" and "Vehicle Cluster Message" as follows:

NFC Cluster Message	Vehicle Cluster Message	Display
To Drive Press Brake And Start Button	X (don't care)	To Drive: Press Brake And Start Button
Scan Digital Key To Drive	X (don't care)	Scan Digital Key To Drive
Scan Digital Key And Press Brake To Shift Gear	X (don't care)	Scan Digital Key And Press Brake To Shift Gear
Digital Key Programming Successful	X (don't care)	Digital Key Programming Successful
Digital Key Programming Fault	X (don't care)	Digital Key Programming Fault
Null	*Any value*	Message specified in "Vehicle Cluster Message" signal

REQ-NFC-ES-312 Driver Information System: "Scan Digital Key And Press Brake To Shift Gear" message details

When the Driver Information System displays the message "Scan Digital Key And Press Brake To Shift Gear", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	Yes: 

REQ-NFC-ES-313 Driver Information System: "Scan Digital Key To Drive" message details

When the Driver Information System displays the message "Scan Digital Key To Drive", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	Yes: 

REQ-NFC-ES-314 Driver Information System: "To Drive: Press Brake And Start" message details

When the Driver Information System displays the message "To Drive: Press Brake And Start Button" message, it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	No

REQ-NFC-ES-315 Driver Information System: "Digital Key Programming Successful" message details

When the Driver Information System displays the message "Digital Key Programming Successful", it shall have the following characteristics:

Message color	Amber

Play chime when message displayed	No
Show icon with message	No

REQ-NFC-ES-316 Driver Information System: "Digital Key Programming Fault" message details

When the Driver Information System displays the message "Digital Key Programming Fault", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	No

REQ-NFC-ES-317 Driver Information System: display time for "To Drive: Press Brake and Start Button" and "Scan Digital Key To Drive"

When any of the following messages are triggered on the Driver Information System:
- "To Drive: Press Brake And Start Button"
- "Scan Digital Key To Drive"

that message shall continue to be displayed until the input signals that caused it to be displayed are changed. After the input signals change, the Driver Information System shall no longer display the message.

REQ-NFC-ES-318 Driver Information System: display time for "Scan Digital Key And Press Brake to Shift Gear" message

After the "Scan Digital Key And Press Brake to Shift Gear" message is triggered, it shall continue to be displayed on the Driver Information System until one of the following occurs:
- The "OK" button is pressed
- The input signals that caused the message to be displayed change their value

When any of the conditions listed above occurs, the Driver Information System shall stop displaying the message immediately.

REQ-NFC-ES-320 Driver Information System: message availability in Limited mode

When the vehicle is in Limited mode (ignition state is not RUN), the following messages shall be displayed if their trigger occurs:
- "To Drive: Press Brake And Start Button"
- "Scan Digital Key To Drive"
- "Digital Key Programming Successful"
- "Digital Key Programming Fault"

3.2 Logical System Properties

3.3 Logical System Requirements

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-311 Driver Information System: message display logic

The Driver Information System shall display warnings based on the "Indication" signal of the "NFC Cluster Message" and "Vehicle Cluster Message" as follows:

NFC Cluster Message	Vehicle Cluster Message	Display
To Drive Press Brake And Start Button	X (don't care)	To Drive: Press Brake And Start Button
Scan Digital Key To Drive	X (don't care)	Scan Digital Key To Drive
Scan Digital Key And Press Brake To Shift Gear	X (don't care)	Scan Digital Key And Press Brake To Shift Gear
Digital Key Programming Successful	X (don't care)	Digital Key Programming Successful
Digital Key Programming Fault	X (don't care)	Digital Key Programming Fault
Null	*Any value*	Message specified in "Vehicle Cluster Message" signal

REQ-NFC-ES-312 Driver Information System: "Scan Digital Key And Press Brake To Shift Gear" message details

When the Driver Information System displays the message "Scan Digital Key And Press Brake To Shift Gear", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	Yes: 

REQ-NFC-ES-313 Driver Information System: "Scan Digital Key To Drive" message details

When the Driver Information System displays the message "Scan Digital Key To Drive", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	Yes: 

REQ-NFC-ES-314 Driver Information System: "To Drive: Press Brake And Start" message details

When the Driver Information System displays the message "To Drive: Press Brake And Start Button" message, it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	No

REQ-NFC-ES-315 Driver Information System: "Digital Key Programming Successful" message details

When the Driver Information System displays the message "Digital Key Programming Successful", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	No

REQ-NFC-ES-316 Driver Information System: "Digital Key Programming Fault" message details

When the Driver Information System displays the message "Digital Key Programming Fault", it shall have the following characteristics:

Message color	Amber
Play chime when message displayed	No
Show icon with message	No

REQ-NFC-ES-317 Driver Information System: display time for "To Drive: Press Brake and Start Button" and "Scan Digital Key To Drive"

When any of the following messages are triggered on the Driver Information System:

- "To Drive: Press Brake And Start Button"
- "Scan Digital Key To Drive"

that message shall continue to be displayed until the input signals that caused it to be displayed are changed. After the input signals change, the Driver Information System shall no longer display the message.

REQ-NFC-ES-318 Driver Information System: display time for "Scan Digital Key And Press Brake to Shift Gear" message

After the "Scan Digital Key And Press Brake to Shift Gear" message is triggered, it shall continue to be displayed on the Driver Information System until one of the following occurs:

- The "OK" button is pressed
- The input signals that caused the message to be displayed change their value

When any of the conditions listed above occurs, the Driver Information System shall stop displaying the message immediately.

REQ-NFC-ES-319 Driver Information System: display time for NFC key programming messages

When any of the following messages are triggered on the Driver Information System:

- "Digital Key Programming Successful"
- "Digital Key Programming Fault"

that message shall be continue to be displayed until any of the following occurs:

- Four seconds elapse from the time the message was triggered
- The OK button is pressed

When either of these conditions are met, the Driver Information system shall stop displaying the message.

-

REQ-NFC-ES-320 Driver Information System: message availability in Limited mode

When the vehicle is in Limited mode (ignition state is not RUN), the following messages shall be displayed if their trigger occurs:

- "To Drive: Press Brake And Start Button"
- "Scan Digital Key To Drive"
- "Digital Key Programming Successful"
- "Digital Key Programming Fault"

4 REVISION HISTORY

Revision	Description	Responsible
2020-08-24	Initial Functional Specification release for UPV1	abonnel1, fehsan2, ekarpins
2020-11-09	Update all functional requirements to reflect latest design. Update behavior diagram for Driver Information System. Add “Vehicle Cluster Message”. Rename “Driver information indication” to “NFC Cluster Message”. Update “NFC Cluster Message” encoding type with new warnings. Remove Nisha Patel from stakeholders list.	abonnel1, fehsan2, ekarpins
2020-11-10	Modified REQ-NFC-ES-319 and REQ-NFC-ES-320 text based on STSS author feedback to align with HMI Global Message List	abonnel1, fehsan2, ekarpins
2021-06-08	Update data dictionary. Add logical architecture information. Updated Figure 3 Added Requirements: • REQ-NFC-ES-312 • REQ-NFC-ES-313 • REQ-NFC-GE2-1 Updated Requirements: • REQ-NFC-ES-311 • REQ-NFC-ES-317	abonnel1, adelong2, fehsan2, ekarpins, jwolf53, rsepulv6
2021-08-06	Requirements and use cases with the prefix REQ-NFC-GE2- are specific to the GE2 programs variant of this feature, and do not appear in this release. If GE2 program-specific information contained in the 2021-06-08 release of this specification replaced other content in the document, the original content is restored.	abonnel1, adelong2, fehsan2, ekarpins, jwolf53, rsepulv6

5 APPENDIX

5.1 Data Dictionary

5.1.1 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.	
Key Type	Digital Key Type		
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		

5.1.2 Logical Parameters

5.1.3 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.

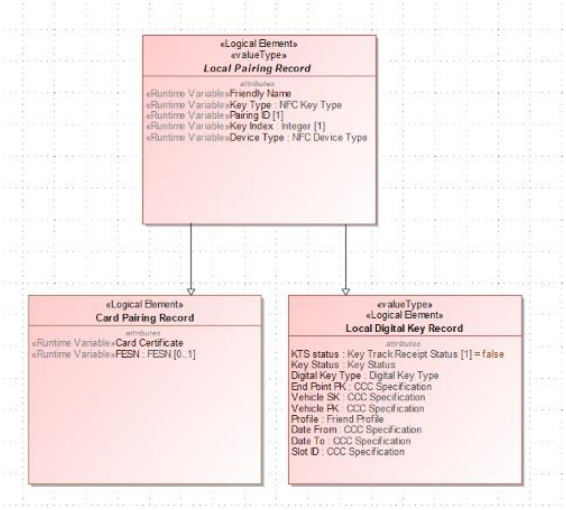
Realized by implementation element:

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

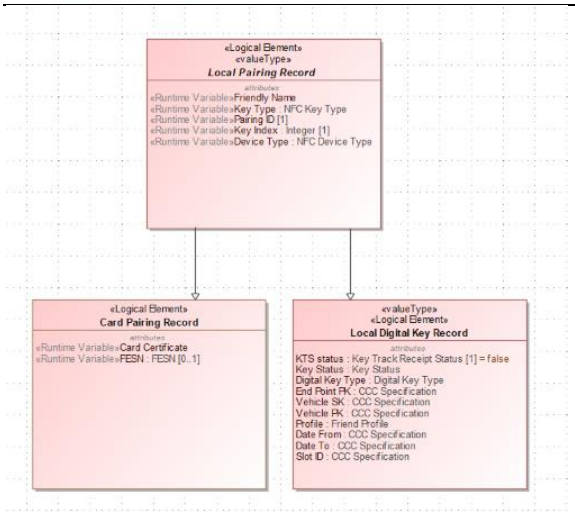
Enumeration Value	Enumeration Value Description
Valid	
Failure	
Awaiting Receipt	
Null	

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	

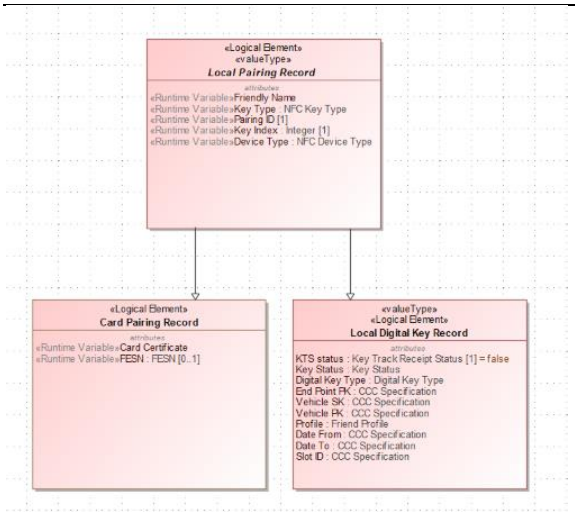
Local ID

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	

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
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.

5.1.4 Technical Signals

5.1.4.1 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	

5.1.5 Technical Parameters

NfcControllerResponseTimeout

Name	NfcControllerResponseTimeout
Description	
Encoding Type	
ECU	APIM

5.2 Glossary

5.2.1 Definitions

No terms specified.

5.2.2 Abbreviations

No acronyms specified.

Document ends here.