Feature – Backup Start Passcode
a.k.a. PaaK Backup

Requirements Specification

Version 2.7
Version Date: June 8, 2018

1 Architectural Design

1.1 Feature Overview

PaaK Backup serves as a backup method for starting vehicles that are equipped with Phone-as-a-Key (PaaK). This feature utilizes the existing keypad entry system as well as a new, password-based starting system. It allows the customer to start and drive away their vehicle even if their phone is not functional (e.g. drained battery) or if their phone is lost, stolen or destroyed. If any of these situations occur, customers can gain entry to the vehicle via the keypad and then use the SYNC HMI to enter a password to prime the vehicle for starting. PaaK Backup also allows customers to generate a temporary password and keypad code to give to valet attendants through an Enhanced Valet Mode in SYNC. This functionality will be integrated into the Valet Mode feature of SYNC.

1.2 Assumptions and Constraints

PaaK Backup will be offered as an opt-in feature. Users may set it up at any time, but they must first activate a phone-as-a-key. PaaK allows users to activate up to four mobile phones as keys. PaaK Backup will allow the customer to associate a unique backup password and keypad code with each of these four phones-as-keys. The BLEM will associate all backup passwords to PaaK key indexes/CAKs authorized for the given vehicle. The valet password will be given a separate key index. The BCM will associate all personalized keypad codes with PaaK key indexes.

Creating and using passwords with PaaK Backup does not require the vehicle to have cloud connectivity. However, cloud connectivity is needed to enhance the security of PaaK Backup. Having connectivity will allow the vehicle to send notifications to the user whenever a password is added, deleted, or used at the vehicle. For PaaK, cloud connectivity to the vehicle and the phone is required to allow the user to revoke their PaaK key remotely. This key revoke action will remove the key from the vehicle as well as remove the backup password and keypad code associated with that key.

The PaaK Backup system is distributed over multiple vehicle subsystems and has functions that are performed by more than one ECU on the vehicle. The BLEM, which is the main controller of the PaaK system, will be responsible for password storage and verification. The BCM will store personal keypad codes and challenge the BLEM when the user attempts to start the vehicle. SYNC will function as the interface for creating and using the passwords. The SYNC module itself will not manage these passwords but rather serve as a pass-through to the BLEM.

Note: This is a list of required CAN signals. See TP APIM/BLEM SPSS for a list of required TP methods.

Sig. ID	Signal Name	Signal Description	Encoding		Min	Max	Tx	Rx
1	IgnPsswrdActv_B_Stat	Password activity status	0x0	Inactive	0 (0x0)	1 (0x1)	BLEM	BCM, APIM
			0x1	Active				
2	IgnPsswrdDsply_B_Rq (wakeup signal)	Password entry screen trigger	0x0	Inactive	0 (0x0)	1 (0x1)	BCM	APIM
			0x1	Active				
3	FobTrgtPssvData_No_Rq	5 bytes of data (challenge data)	Unitless		0 (0x0)	1099511627775 (0xFFFFFFFFFF)	BLEM	BCM
4	FobCtlPssvData_No_Actl	5 bytes of data (response data)	Unitless		0 (0x0)	1099511627775 (0xFFFFFFFFFF)	BCM	BLEM
5	FobTrgtType_D_Rq	Type of search being requested	0x0	Null	0 (0x0)	7 (0x7)	BLEM	BCM
			0x1	Crypto				
			0x2	Registry				
			0x3	Polling				
			0x4 - 0x7	*NotUsed*				
6	FobCtlType_D_Stat	Indication of whether a valid key fob was found during the last search	0x0	Null	0 (0x0)	3 (0x3)	BCM	BLEM
			0x1	Invalid				
			0x2	Valid				
			0x3	*NotUsed*				
7	FobTrgtZone_D_Rq	Indication of the zone in or around the vehicle to be searched	0x0	Null	0 (0x0)	15 (0xF)	BLEM	BCM
			0x1	Interior				
			0x2	Driver				
			0x3	Passenger				
			0x4	RearExterior				
			0x5	RearInterior				
			0x6	Approach				
			0x7 - 0xF	*Reserved*				
8	FobTrgtRollCode_No_Rq	Rolling count transmitted by the Target function to align a search request with the corresponding search result		Unitless	0 (0x0)	15 (0xF)	BLEM	BCM

9	FobCtlRollCode_No_Stat	Rolling count transmitted by the Control function to align a search request with the corresponding search result		Unitless	0 (0x0)	15 (0xF)	BCM	BLEM
10	IgnPsswrdSetup_B_Rq	Signal used to trigger LBI setup	0x0	Inactive	0 (0x0)	1 (0x1)	BLEM	APIM
			0x1	Active				
11	IgnPsswrdLckout_B_Stat	Signal used to enable lockout	0x0	Inactive	0 (0x0)	1 (0x1)	BLEM	APIM
			0x1	Active				
12	KeyPadCodeProg_D_Rq	Signal used to trigger KeyPad Code Add/Delete request	0x0	Null	0 (0x0)	4 (0x4)	BLEM	BCM
			0x1	ProgrammingMode				
			0x2	Add				
			0x3	Delete				
			0x4	DeleteAll				
13	KeyPadCodeProg_D_Stat	Signal indicating status for Keypad Code Add/Delete request	0x0	NormalMode	0 (0x0)	5 (0x5)	BCM	BLEM
			0x1	LearningMode				
			0x2	Add				
			0x3	Delete				
			0x4	DeleteAll				
			0x5	ProgrammingFailure				
			0x6	Duplicate				
14	PaakTrgtActvData_No_Rq	RKE Challenge Data		Unitless	0 (0x0)	1099511627775 (0xFFFFFFFFFF)	BCM	BLEM
15	PaakCtlActvData_No_Actl	RKE Response Data		Unitless	0 (0x0)	1099511627775 (0xFFFFFFFFFF)	BLEM	BCM
16	PaaKCtlActv_No_Actl	Phone SubID		Unitless	0 (0x0)	63 (0x3F)	BLEM	BCM
17	PaakTrgtType_D_Rq	Type of search being requested	0x0	Null	0 (0x0)	7 (0x7)	BCM	BLEM
			0x1	Crypto				
			0x2	Registry				
			0x3	Polling				
18	GearLvrPos_D_Actl	Gear lever State	0x0	Park	0 (0x0)	63 (0x3F)	TCM	BLEM/ APIM
			0x1	Reverse				
			0x2	Neutral				
			0x3	Drive				
			0x4	Sport_DriveSport				
			0x5	Low				
			0x6	First				
			0x7	Second				
			0x8	Third				
			0x9	Fourth				
			0xA	Fifth				
			0xB	Sixth				

			0xC	Undefined_Treat_as_Fault				
			0xD	Undefined_Treat_as_Fault				
			0xE	Unknown_Position				
			0xF	Fault				
19	Ignition_Status	Status of Ignition	0x0	Unknown	0 (0x0)	15 (0xF)	BCM	BLEM/ APIM
			0x1	Off				
			0x2	Accessory				
			0x4	Run				
			0x8	Start				
			0xF	Invalid				
20	FactoryReset_Rq	Factory Reset Defaults	0x0	Inactive	0 (0x0)	1 (0x1)	APIM	BLEM
			0x1	ResetFactoryDefaults				
21	Delay_Accy	Delayed Accessory Mode	0x0	Off	0 (0x0)	1 (0x1)	BCM	APIM
			0x1	On				
22	ModemReset_D_Rq	Modem reset	0x0	Null	0 (0x0)	15 (0xF)	APIM	BLEM
			0x1	WifiHotSpot_Reset				
			0x2	Paak_Reset				
			0x3	Online_Traffic_Reset				
			0x4	CCS_Reset				
			0x5 - 0xF	NotUsed				
23	PwPckTq_D_Stat	Motive/Non-motive vehicle status	0x00	PwPckOff_TqNotAvailable	0 (0x0)	3 (0x3)	PCM	APIM
			0x01	PwPckOn_TqNotAvailable				
			0x02	StartInPrgrss_TqNotAvailable				
			0x03	PwPckOn_TqAvailable				

2 Functional Definition

Note: The actual Marketing names for PaaK and PaaK Backup are yet to be determined. References to PaaK and PaaK Backup are for descriptive purposes.

2.1 Primary Functions

2.1.1 Creating backup password and keypad code for PaaK device

2.1.1.1 Requirements

[LBI.R001.03] The BLEM shall keep track of whether PaaK devices in the vehicle have an associated backup password. If the BLEM detects one such device while ignition is in Run (*Ignition_Status = 0x4 = Run*) and transmission is in Park (*GearLvlPos_D_Actl = 0x0 = Park*), it shall notify SYNC (*IgnPsswrdSetup_B_Rq = 0x1 = Active*) *five times,* once per ignition cycle, per lifetime of the CAK associated with that device.

[LBI.R002.02] When SYNC receives *IgnPsswrdSetup_B_Rq = 0x1 = Active* from the BLEM, the SYNC HMI shall display a message to the user with the option to create a backup password.

[LBI.R003.03] When the user selects the option to create a backup password, the SYNC HMI shall display a screen with requirements and steps to create a backup password.

[LBI.R330.01] When user chooses to continue, then SYNC shall query the BLEM for PaaK devices without passwords in the vehicle and shall request the cryptographic salt (*BackupIgnition_Rq* with *OpCode = 0x04 = Salt and Check for PaaK without Passwords, Byte 5 = 0x00*).

[LBI.R183.02] The BLEM shall trigger a BCM Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*) whenever it receives *BackupIgnition_Rq* with *OpCode = 0x04 = Salt and Check for PaaK without Passwords.*

Note: *The encrypted data is used to authenticate searches. The roll code is used to synchronize the request and response.*
See details of BCM Interior Registry search in Section 3.1.4

[LBI.R184.02] After completing BLEM-requested Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*), the BCM shall report to the BLEM whether any key fobs were detected in the vehicle (*FobCtlType_D_Stat, FobCtlPssvData_No_Actl, FobCtlRollCode_No_Stat*).

[LBI.R006.02] After receiving Interior Registry search results from the BCM, the BLEM shall report to SYNC what devices (PaaK w/o passwords or key fob) were found in the vehicle, the names and key indexes of all PaaK devices found in the vehicle, as well as the cryptographic salt (*BackupIgnition_Rsp* with *RspCode = 0x04 = Salt and Check for PaaK without Passwords Response*).

Note: *Name here refers to the device name generated during PaaK setup.*

[LBI.R007.02] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x04 = Salt and Check for PaaK without Passwords Response*, the SYNC HMI shall display either:

1. Error message that lists key fob as missing with options to retry or cancel if:
    - *RspStatus = 0x02 = One PaaK w/o Password and No Fob In Vehicle* OR
    - *RspStatus = 0x05 = Two+ PaaK w/o Password and No Fob In Vehicle* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
2. Error message that lists phone as missing with options to retry or cancel if:
    - *RspStatus = 0x03 = Fob In Vehicle and No PaaK* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
3. Error message that lists key fob and phone as missing with options to retry or cancel if:
    - *RspStatus = 0x06 = No PaaK w/o Password and No Fob In Vehicle* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
4. Backup password creation screen if:
    - *RspStatus = 0x01 = One PaaK w/o Password and Fob In Vehicle* AND
    - *Byte 6 = 0x01, Challenge Nonce = EOS, Salt = Salt, Valet Password = EOS, KeyIndex = KeyIndex, PhoneName = PhoneName*
5. List of all detected PaaK devices with instruction for the user to choose the desired device if:
    - *RspStatus = 0x04 = Two+ PaaK w/o Password and Fob In Vehicle* AND
    - *Byte 6 = 0x02 - 0x04, Challenge Nonce = EOS, Salt = Salt, Valet Password = EOS, KeyIndex = KeyIndex, PhoneName = PhoneName*

[LBI.R008.02] When the user chooses their desired device from the list, the SYNC HMI shall display the backup password creation screen.

[LBI.R009.02] The SYNC HMI shall require the user to enter their new backup password twice. If passwords do not match, the SYNC HMI shall notify the user and provide an option to retry.

[LBI.R010.02] SYNC shall check entered passwords against password requirements in real time. The SYNC HMI shall not allow the user to proceed to the next screen until their password meets the minimum requirements.

[LBI.R011.03] SYNC shall compute a hash of the entered password and send the result to the BLEM with the key index of the selected device (*BackupIgnition_Rq* with *OpCode = 0x07 = Password Transmit, KeyIndex = KeyIndex, Password = Password, KeypadCode = EOS*).

[LBI.R012.03] Upon receiving the password hash and key index (*BackupIgnition_Rq* with *OpCode = 0x07 = Password Transmit*), the BLEM shall trigger a BCM Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*).

[LBI.R185.02] After completing BLEM-requested Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*),

the BCM shall report to the BLEM whether any key fobs were detected in the vehicle (*FobCtlType_D_Stat, FobCtlPssvData_No_Actl, FobCtlRollCode_No_Stat*).

[LBI.R013.02] After receiving Interior Registry search results from the BCM, the BLEM shall respond to SYNC with *BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response* and either

1. *RspStatus = 0x08 = Fob No Longer Detected* if:
    - The BCM does not detect a key fob in the vehicle (*FobCtlType_D_Stat = 0x1 = Invalid*) AND
    - The BLEM detects the PaaK device associated with the received key index.
2. *RspStatus = 0x07 = PaaK No Longer Detected* if:
    - The BCM detects a key fob in the vehicle (*FobCtlType_D_Stat = 0x2 = Valid*) AND
    - The BLEM does not detect the PaaK device associated with the received key index
3. *RspStatus = 0x09 = PaaK and Fob No Longer Detected* if:
    - The BCM does not detect a key fob in the vehicle (*FobCtlType_D_Stat = 0x1 = Invalid*) AND
    - The BLEM does not detect the PaaK device associated with the received key index

Note: See details of BCM Interior Registry search in Section 3.1.4

[LBI.R186.01] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response*, the SYNC HMI shall display either:

1. Error message that lists key fob as missing with options to retry (restart the process) or cancel. if:
    - *RspStatus = 0x08 = Fob No Longer Detected* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
2. Error message that lists phone as missing with options to retry (restart the process) or cancel. if:
    - *RspStatus = 0x07 = PaaK No Longer Detected* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
3. Error message that lists key fob and phone as missing with options to retry (restart the process) or cancel if:
    - *RspStatus = 0x09 = PaaK and Fob No Longer Detected* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*

[LBI.R014.02] If the PaaK device that the user selected and a key fob are still in the vehicle when the BLEM receives the password hash, the BLEM shall verify that the entered password is not already being used.

[LBI.R187.01] If the BLEM determines that the password is already being used, the BLEM shall notify SYNC of this (*BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response, RspStatus = 0x0A = Password Already Used, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R188.01] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response, RspStatus = 0x0A = Password Already Used,* the SYNC HMI shall display a message that password is already being used and instruct user to enter a different password.

[LBI.R015.02] If the BLEM determines that password is not already being used, the BLEM shall store the password hash in its HSM and associate it with the received key index.

[LBI.R331.01] When the BLEM cannot store the password hash in its HSM, it shall notify SYNC (*BackupIgnition_Rsp with RspCode = 0x07 = Password Response, RspStatus = 0x0C = Password Created Failed, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R332.01] When SYNC receives creation failure response (*BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response, RspStatus = 0x0C = Password Created Failed*), the SYNC HMI shall notify user of unsuccessful password creation.

[LBI.R189.03] When the BLEM stores a new password hash, it shall report this to the TCU (*LBIAlert_St* with *Event = 0x01 = Backup Password Created, Source = 0x00, [timestamp], [Key ID]*) in a BLEM SyncP signed packet (Service Type 0x40/Sub-Service 0x0) as defined in Transfer Protocol BLEM SPSS.

Note: *Reference TP BLEM SPSS and LBI SPSS for BLEM SyncPPacket definition and its payload. Key ID here refers to the Key ID of the PaaK device associated with the created backup password.*

[LBI.R190.01] When the BLEM stores a new password hash, it shall report this to SYNC (*BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response, RspStatus = 0x0B = Password Created Successfully, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R191.01] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x07 = Password Response, RspStatus = 0x0B = Password Created Successfully*, the SYNC HMI shall notify the user of successful backup password creation.

[LBI.R016.01] After creating backup password, the SYNC HMI shall present the user with the option to set up a personal keypad code.

[LBI.R017.02] If the user chooses not to create a personal keypad code, the SYNC HMI shall inform the user that PaaK Backup setup is complete and provide instructions on how to use the feature.

[LBI.R018.02] If the user chooses to create a personal keypad code, the SYNC HMI shall display a screen for entering a new personal keypad code.

[LBI.R019.01] The SYNC HMI shall require the user to enter their new personal keypad code twice.

[LBI.R192.01] SYNC shall verify that the two codes entered match. If the codes do not match, the SYNC HMI shall notify the user and provide an option to retry.

[LBI.R020.02] If the codes match, SYNC shall send to the BLEM the keypad code, the key index of the selected PaaK device, and a request to store the keypad code (*BackupIgnition_Rq* with *OpCode = 0x08 = Keypad Code Create Request, KeyIndex = KeyIndex, Password = EOS, KeypadCode = KeypadCode*).

[LBI.R021.02] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x08 = Keypad Code Create Request, KeyIndex = KeyIndex, Password = EOS, KeypadCode = KeypadCode*, it shall respond (*PaaKCtlActvData_No_Actl*) to periodic RKE challenge from the BCM (*PaaKTrgtActvData_No_Rq*) and send a request to the BCM to enter keypad programming mode (*KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode*).

Note: See details of BLEM-BCM Keypad programming requirements in Section 3.1.5

[LBI.R022.03] When the BCM receives *KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode* together with valid RKE response data from the BLEM, it shall enter keypad programming mode and notify the BLEM (*KeyPadCodeProg_D_Stat = 0x2 = LearningMode*) within two seconds and remain in programming mode/provide notification for up to two seconds.

[LBI.R023.02] When the BLEM receives *KeyPadCodeProg_D_Stat = 0x2 = LearningMode*, it shall send to the BCM the received keypad code (in *PaaKCtlActvData_No_Actl*), the received key index (*PaaKCtlActv_No_Actl = [index]*) and a request to store the personal keypad code (*KeyPadCodeProg_D_Rq = 0x2 = Add*).

[LBI.R024.02] When the BCM receives the request to store the personal keypad code (*KeyPadCodeProg_D_Rq = 0x2 = Add*) together with the key index (*PaaKCtlActv_No_Actl = [index]*) and the keypad code (in *PaaKCtlActvData_No_Actl*), it shall store the received keypad code and associate it with the received key index.

[LBI.R193.01] When the BCM stores a new keypad code, it shall notify the BLEM (*KeyPadCodeProg_D_Stat = 0x3 = Add*) for one second and then exit programming mode (*KeyPadCodeProg_D_Stat = 0x0 = NormalMode*).

[LBI.R302.01] When the BCM cannot store a new keypad code, it shall notify the BLEM (*KeyPadCodeProg_D_Stat = 0x5 = ProgrammingFailture*) for one second and then exit programming mode (*KeyPadCodeProg_D_Stat = 0x0 = NormalMode*).

[LBI.R025.03] When the BLEM receives confirmation of keypad code storage (*KeyPadCodeProg_D_Stat = 0x3 = Add*), it shall:

- Update keypad code association status for selected/detected key index
- Notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x08 = Keypad Code Create Response, RspStatus = 0x0D = Keypad Code Created Successfully, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R194.01] When SYNC receives confirmation of keypad code storage (*BackupIgnition_Rsp* with *RspCode = 0x08 = Keypad Code Create Response, RspStatus = 0x0D = Keypad Code Created Successfully*), the SYNC HMI shall notify the user of successful keypad code creation.

[LBI.R333.01] After SYNC notifies user of successful keypad code creation, it shall inform user that PaaK Backup setup is complete and provide instructions on how to use the feature.

[LBI.R303.01] When the BLEM receives programming failure response (*KeyPadCodeProg_D_Stat = 0x3 = 0x5 = ProgrammingFailure*), it shall notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x08 = Keypad Code Create Response, RspStatus = 0x0E = Keypad Code Created Failed, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R304.01] When SYNC receives programming failure response (*BackupIgnition_Rsp* with *RspCode = 0x08 = Keypad Code Create Response, RspStatus = 0x0E = Keypad Code Created Failed*), the SYNC HMI shall notify user of programming failure.

2.1.1.2 Use Case

2.1.1.2.1 Creating backup password and keypad code for PaaK device

Actors	User
Pre-conditions	User has previously activated Phone-as-a-Key feature for vehicle. Vehicle is in RUN. User is inside vehicle. One associated PaaK device and key fob are inside the vehicle.
Scenario Description	1. User selects option to Create Backup Password for Phone-as-a-Key from PaaK Backup Settings in SYNC.

	2. SYNC displays screen with creation steps. 3. SYNC displays alphanumeric password entry screen and instructs user to enter a backup password. 4. User enters password twice according to password requirements. 5. User selects Enter. 6. SYNC displays message that backup password has been created successfully. SYNC also asks user if they would like to create a personal keypad code. 7. User selects option to create a personal keypad code. 8. SYNC displays screen for entering personal keypad code. 9. User enters personal keypad code twice. 10. SYNC displays message that new personal keypad code has been created successfully.
Post-conditions	PaaK Backup is ready for use. Notification that backup password has been created is sent to user.
List of Exceptions	User enters password that does not meet requirements. User enters passwords that do not match. User enters passwords that is already in use.
Interfaces	APIM BCM BLEM TCU SDN PaaK FI

2.1.2 Starting vehicle with backup password

2.1.2.1 Requirements

[LBI.R026.02] The BCM shall notify SYNC (*IgnPsswrdDsply_B_Rq = 0x1 = Active*) whenever:

1. The user presses the start button or the brake pedal AND
2. No key fobs or phones-as-keys are detected in the vehicle AND
3. There is at least one backup password created (*IgnPsswrdActv_B_Stat = 0x1 = Active*).

[LBI.R027.04] When SYNC receives *IgnPsswrdDsply_B_Rq = 0x1 = Active* and *Ignition_Status = 0x1 = Off* and the status of Enhanced Valet Mode in SYNC is inactive, SYNC shall enter Infotainment Mode and display either:

1. A backup password entry screen if *IgnPsswrdLckout_B_Stat = 0x0 = Inactive* OR
2. A lockout popup if *IgnPsswrdLckout_B_Stat = 0x1 = Active*

[LBI.R197.02] When the user enters a password at the backup password entry screen, SYNC shall request a challenge from the BLEM (*BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request, Byte 5 = 0x00*).

[LBI.R198.01] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request*, it shall issue a challenge to SYNC with cryptographic nonce and salt (*BackupIgnition_Rsp* with *RspCode = 0x01 = Issue Challenge, RspStatus = 0x00 = Reserved, Byte 6 = 0x00, Challenge Nonce = Challenge Nonce, Salt = Salt, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R199.01] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request*, it shall compute, using the cryptographic nonce, another hash of all stored password hashes.

[LBI.R031.02] SYNC shall compute a hash of entered password using received salt and then compute a hash of this result using received nonce.

[LBI.R032.02] SYNC shall respond to the challenge from the BLEM (*BackupIgnition_Rsp* with *RspCode = 0x01 = Issue Challenge*) with computed password hash (*BackupIgnition_Rq* with *OpCode = 0x02 = Challenge Response, KeyIndex = EOS, Password = Challenge Password, KeypadCode = EOS*).

[LBI.R033.01] When the BLEM receives a challenge hash from SYNC (*BackupIgnition_Rq* with *OpCode = 0x02 = Challenge Response, KeyIndex = EOS, Password = Challenge Password, KeypadCode = EOS*), it shall compare it with the hashes that it computed for the stored passwords.

[LBI.R034.03] If the BLEM determines that the received password is valid i.e. challenge hash matches a calculated password hash, it shall notify SYNC of this (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x0F = Valid Password, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*) and start a 21-second authorization period.

[LBI.R307.02] When the BLEM is in a 21-second authorization period while *Ignition_Status = 0x1 = Off*, the BLEM shall respond positively (*PaakCtlType_D_Stat = 0x2 = Valid, PaakCtlIndx1_No_Actl = [Index]*) to BCM Crypto Start searches (*PaakTrgtType_D_Rq = 0x1 = Crypto, PaakTrgtZone_D_Rq = 0x1 = Interior)*, but negatively to Registry or Polling searches. After this period expires, the BLEM shall respond negatively (*PaakCtlType_D_Stat = 0x1 = Invalid*) to BCM Crypto Start searches.

Note: The index that the BLEM sends is the key index of the PaaK device that the entered password is associated with.

[LBI.R200.03] When the BLEM responds positively to a Crypto Start search during 21-second authorization period and it is not in Enhanced Valet Mode, it shall report this to the TCU (*LBIAlert_St* with *Event = 0x02 = Backup Password Used, Source = 0x00, [timestamp], [Key ID]*) in a BLEM SyncP signed packet (Service Type 0x40/Sub-Service 0x0) as defined in Transfer Protocol BLEM SPSS.

Note: *Reference TP BLEM SPSS and LBI SPSS for BLEM SyncPPacket definition and its payload. Key ID here refers to the Key ID of the PaaK device associated with the entered backup password.*

[LBI.R035.02] When SYNC receives a valid notification from the BLEM (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x0F = Valid Password*), the SYNC HMI shall notify the user that the entered password has been accepted and that they must start the vehicle now. This message shall display for 20 seconds unless vehicle ignition status changes to Run (*Ignition_Status = 0x4 = Run*), then this message shall be dismissed.

[LBI.R036.02] If the BLEM determines that the received password is invalid i.e. challenge hash does not match a calculated password hash, it shall increment invalid password counter and then notify SYNC (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x10 = Invalid Password, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R037.03] When SYNC receives an invalid password notification (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x10 = Invalid Password*), the SYNC HMI shall notify the user that the entered password is invalid and provide an option to retry.

[LBI.R038.01] The BLEM shall keep track of invalid attempts at entering the backup password and invalid attempts at entering the valet password in separate counters.

[LBI.R201.03] Invalid attempt counters shall be stored in NVM and shall not be reset by change in vehicle ignition status, network status, or battery state of charge.

[LBI.R039.01] The backup password counter shall be reset each time a backup password is successfully entered. The valet password counter shall be reset each time a valet password is successfully entered or Enhanced Valet Mode is exited.

[LBI.R040.03] If either attempt counter reaches five invalid attempts, the BLEM shall start a five minute timer and notify SYNC of lockout (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x19 = Lockout, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*) and send out *IgnPsswrdLckout_B_Stat = Active* until timer expires.

[LBI.R407.01] When the BLEM initiates a five minute lockout timer it shall ignore any incoming opcode requests until lockout timer expires.

[LBI.R308.02] When the BLEM starts a lockout timer, it shall report this to the TCU (*LBIAlert_St* with *Event = 0x07 = Lockout, Source = 0x00, [timestamp], [Key ID]*) in a BLEM SyncP signed packet (Service Type 0x40/Sub-Service 0x1) as defined in Transfer Protocol BLEM SPSS.

Note: *Reference TP BLEM SPSS and LBI SPSS for BLEM SyncPPacket definition and its payload. Key ID here should be left blank, zero. This is a "notify all" alert since it is impossible to determine which Key ID is being used if invalid passwords are continuously entered. No Key ID's can be contained since it is not possible to know which one is the primary target, so this alert needs to be sent out to users of all PaaK devices.*

[LBI.R202.03] Lockout timer shall be stored in NVM and shall not be reset by change in vehicle ignition status, network status, or battery state of charge.

[LBI.R334.01] During these five minutes, whenever the user attempts to use a password to start the vehicle, exit secure idle, reset a current password, or activate/deactivate Enhanced Valet Mode, the SYNC HMI shall display a screen with information that password entry has been locked out.

[LBI.R041.02] Lockout shall occur every time the attempt counter reaches five invalid attempts.

2.1.2.2 Use Case

2.1.2.2.1 Starting vehicle with backup password

Actors	User
Pre-conditions	User has previously created a backup password. Vehicle is locked. User is outside vehicle. No associated key fobs or phones-as-keys are near the vehicle.

Scenario Description	1. User approaches vehicle. 2. User enters valid keypad code. 3. Vehicle unlocks. 4. User opens door and enters vehicle. 5. User presses brake pedal. 6. SYNC displays backup password entry screen. 7. Without being inactive for more than 30 seconds, user enters valid backup password via SYNC. (This includes inputting the password then selecting Enter.) 8. SYNC displays message instructing user to start the vehicle. 9. Within 20 seconds, user presses start button while holding brake pedal. 10. Vehicle starts with engine running.
Post-conditions	User is able to drive away vehicle. User is able to charge their PaaK device in vehicle. Notification that PaaK Backup has been used is sent to user.
List of Exceptions	User does not enter valid keypad code. User does not enter valid password. User is inactive for more than 30 seconds while SYNC displays password entry screen. User does not start vehicle within 20 seconds of successful password entry. User presses start button without holding brake pedal after password is accepted.
Interfaces	APIM BCM BLEM TCU SDN PaaK FI

2.1.3 Deleting backup password and keypad code for PaaK device

2.1.3.1 Requirements

[LBI.R042.02] When the user selects the option to delete a backup password within SYNC settings, SYNC shall query the BLEM for PaaK devices with passwords in the vehicle and shall request the cryptographic salt (*BackupIgnition_Rq* with *OpCode = 0x03 = Salt and Check for PaaK with Passwords, Byte 5 = 0x00*).

[LBI.R203.02] The BLEM shall trigger a BCM Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*) whenever it receives *BackupIgnition_Rq* with *OpCode = 0x03 = Salt and Check for PaaK with Passwords*.

Note: See details of BCM Interior Registry search in Section 3.1.4

[LBI.R204.02] After completing BLEM-requested Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*), the BCM shall report to the BLEM whether any key fobs were detected in the vehicle (*FobCtlType_D_Stat, FobCtlPssvData_No_Actl, FobCtlRollCode_No_Stat*).

[LBI.R205.02] After receiving Interior Registry search results from the BCM, the BLEM shall report to SYNC what devices (PaaK with passwords or key fob) were found in the vehicle, the names and key indexes of all PaaK devices found in the vehicle, as well as the cryptographic salt (*BackupIgnition_Rsp* with *RspCode = 0x03 = Salt and Check for PaaK with Passwords Response*).

[LBI.R043.02] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x03 = Salt and Check for PaaK with Passwords Response*, the SYNC HMI shall display either:

1. Error message that lists phone as missing with options to retry or cancel if:
    - *RspStatus = 0x13 = Fob In Vehicle and No PaaK w/ Password* OR
    - *RspStatus = 0x16 = No PaaK w/ Password and No Fob In Vehicle* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
2. List of all detected PaaK devices with instruction for the user to choose the desired device if:
    - *RspStatus = 0x11 = One PaaK w/ Password and Fob In Vehicle* OR
    - *RspStatus = 0x12 = One PaaK w/ Password and No Fob In Vehicle* OR
    - *RspStatus = 0x14 = Two+ PaaK w/ Password and Fob In Vehicle* OR
    - *RspStatus = 0x15 = Two+ PaaK w/ Password and No Fob In Vehicle* AND
    - *Byte 6 = 0x01 – 0x04, Challenge Nonce = EOS, Salt = Salt, Valet Password = EOS, KeyIndex = KeyIndex, PhoneName = PhoneName*

[LBI.R046.03] When the user chooses their desired device (password) for deletion, the SYNC HMI shall ask the user to confirm deletion of the associated password.

[LBI.R047.03] When the user confirms deletion of their password, SYNC shall send to the BLEM the key index of the selected PaaK device together with a request to delete the password hash associated with this key index (*BackupIgnition_Rq* with *OpCode = 0x09 = Password Delete Request, KeyIndex = KeyIndex, Password = EOS, KeypadCode = EOS*).

[LBI.R048.03] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x09 = Password Delete Request, KeyIndex = KeyIndex, Password = EOS, KeypadCode = EOS*, it shall immediately delete the password hash associated with the received key index.

[LBI.R206.03] When the BLEM deletes a backup password hash, it shall report this to the TCU (*LBIAlert_St* with *Event = 0x03 = Backup Password Deleted, Source = 0x00, [timestamp], [Key ID]*) in a BLEM SyncP signed packet (Service Type 0x40/Sub-Service 0x0) as defined in Transfer Protocol BLEM SPSS.

Note: *Reference TP BLEM SPSS and LBI SPSS for BLEM SyncPPacket definition and its payload. Key ID here refers to the Key ID of the PaaK device associated with the deleted backup password.*

[LBI.R207.02] When the BLEM deletes a backup password hash, it shall also determine whether there is a keypad code associated with the received key index.

Note: See details of BLEM-BCM Keypad programming requirements in Section 3.1.5

If there is an associated keypad code, the BLEM shall initiate keypad code deletion by responding (with *PaaKCtlActvData_No_Actl*) to periodic RKE challenge from the BCM (*PaaKTrgtActvData_No_Rq*) and sending a request to the BCM to enter keypad programming mode (*KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode*).

If there is no associated keypad code, the BLEM shall notify SYNC of successful deletion (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x17 = Password Deleted Successfully, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R335.01] When the BLEM cannot delete the backup password hash, it shall notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x18 = Password Deleted Failed, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R336.01] When SYNC receives deletion failure response (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x18 = Password Deleted Failed*), the SYNC HMI shall notify user of unsuccessful password deletion.

[LBI.R049.03] When the BCM receives *KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode* together with valid RKE response data from the BLEM, it shall enter keypad programming mode and notify the BLEM (*KeyPadCodeProg_D_Stat = 0x2 = LearningMode*) within two seconds and continue to provide notification for up to two seconds.

[LBI.R050.02] When the BLEM receives *KeyPadCodeProg_D_Stat = 0x2 = LearningMode*, it shall send to the BCM the received key index (*PaaKCtlActv_No_Actl = [index]*) and a request to delete the personal keypad code (*KeyPadCodeProg_D_Rq = 0x3 = Delete*).

[LBI.R051.02] When the BCM receives the request to delete the personal keypad code (*KeyPadCodeProg_D_Rq = 0x3 = Delete*) together with the key index (*PaaKCtlActv_No_Actl = [index]*), it shall delete the personal keypad code that is associated with the received key index.

[LBI.R208.01] When the BCM deletes a keypad code, it shall notify the BLEM (*KeyPadCodeProg_D_Stat = 0x4 = Delete*) for one second and then exit programming mode (*KeyPadCodeProg_D_Stat = 0x0 = NormalMode*).

[LBI.R309.01] When the BCM cannot delete a new keypad code, it shall notify the BLEM (*KeyPadCodeProg_D_Stat = 0x5 = ProgrammingFailture*) for one second and then exit programming mode (*KeyPadCodeProg_D_Stat = 0x0 = NormalMode*).

[LBI.R052.02] When the BLEM receives confirmation of keypad code deletion (*KeyPadCodeProg_D_Stat = 0x4 = Delete*), it shall notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x17 = Password Deleted Successfully, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R209.01] When SYNC receives confirmation of keypad code deletion (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x17 = Password Deleted Successfully*), the SYNC HMI shall notify the user of successful password (and keypad code, if applicable) deletion.

[LBI.R310.02] When the BLEM receives programming failure response (*KeyPadCodeProg_D_Stat = 0x5 = ProgrammingFailure*), it shall notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x1E = Password Deleted Successfully, but Keypad Code Deleted Failed, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R311.02] When SYNC receives programming failure response (*BackupIgnition_Rsp* with *RspCode = 0x09 = Password Delete Response, RspStatus = 0x1E = Password Deleted Successfully, but Keypad Code Deleted Failed*), the SYNC HMI shall notify user of successful password deletion and unsuccessful keypad code deletion.

2.1.3.2 Use Case

Actors	User
Pre-conditions	Vehicle is in RUN. User is inside vehicle. One associated PaaK device with password is inside the vehicle.
Scenario Description	1. User selects option to Delete Backup Password for Phone-as-a-Key from PaaK Backup Settings in SYNC. 2. SYNC displays message with deletion requirements. 3. User continues. 4. SYNC displays message asking user if they are sure they want to delete their password and personal keypad code. 5. User confirms. 6. SYNC displays message that backup password and personal keypad code have been deleted successfully.
Post-conditions	Notification that backup password has been deleted is sent to user.
List of Exceptions	
Interfaces	APIM BCM BLEM TCU SDN PaaK FI

2.1.4 Resetting backup password and keypad code for PaaK device

2.1.4.1 Requirements

[LBI.R053.02] When the user selects the option to reset a backup password within SYNC settings, SYNC shall query the BLEM for PaaK devices with passwords in the vehicle and shall request the cryptographic salt (*BackupIgnition_Rq* with *OpCode = 0x03 = Salt and Check for PaaK with Passwords, Byte 5 = 0x00*).

[LBI.R210.02] The BLEM shall trigger a BCM Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*) whenever it receives *BackupIgnition_Rq* with *OpCode = 0x03 = Salt and Check for PaaK with Passwords*.

Note: See details of BCM Interior Registry search in Section 3.1.4

[LBI.R211.02] After completing BLEM-requested Interior Registry search (*FobTrgtType_D_Rq = 0x2 = Registry, FobTrgtZone_D_Rq = 0x1 = Interior, FobTrgtPssvData_No_Rq, FobTrgtRollCode_No_Rq*), the BCM shall report to the BLEM whether any key fobs were detected in the vehicle (*FobCtlType_D_Stat, FobCtlPssvData_No_Actl, FobCtlRollCode_No_Stat*).

[LBI.R054.03] After receiving Interior Registry search results from the BCM, the BLEM shall report to SYNC what devices (PaaK with passwords or key fob) were found in the vehicle, the names and key indexes of all PaaK devices with passwords found in the vehicle, as well as the cryptographic salt (*BackupIgnition_Rsp* with *RspCode = 0x03 = Salt and Check for PaaK with Passwords Response*).

[LBI.R055.02] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x03 = Salt and Check for PaaK with Passwords Response*, the SYNC HMI shall display either:

1. Error message that lists phone as missing with options to retry or cancel if:
    - *RspStatus = 0x13 = Fob In Vehicle and No PaaK w/ Password* OR
    - *RspStatus = 0x16 = No PaaK w/o Password and No Fob In Vehicle* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
2. List of all detected PaaK devices with instruction for the user to choose the desired device if:
    - *RspStatus = 0x11 = One PaaK w/ Password and Fob In Vehicle* OR
    - *RspStatus = 0x12 = One PaaK w/ Password and No Fob In Vehicle* OR
    - *RspStatus = 0x14 = Two+ PaaK w/ Password and Fob In Vehicle* OR
    - *RspStatus = 0x15 = Two+ PaaK w/ Password and No Fob In Vehicle* AND

- *Byte 6 = 0x01 – 0x04, Challenge Nonce = EOS, Salt = Salt, Valet Password = EOS, KeyIndex = KeyIndex, PhoneName = PhoneName*

[LBI.R212.02] When the user chooses their desired device (password) for resetting, the SYNC HMI shall display either:

1. The backup password entry screen (to start Reset Option 1) if:
   - *RspStatus = 0x12 = One PaaK w/ Password and No Fob In Vehicle* OR
   - *RspStatus = 0x15 = Two+ PaaK w/ Password and No Fob In Vehicle*
2. The backup password creation screen (to start Reset Option 2) if:
   - *RspStatus = 0x11 = One PaaK w/ Password and Fob In Vehicle* OR
   - *RspStatus = 0x14 = Two+ PaaK w/ Password and Fob In Vehicle*

Reset Option 1 starts here.

[LBI.R213.02] When the user enters a password at the backup password entry screen, SYNC shall request a challenge from the BLEM (*BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request, Byte 5 = 0x00*).

[LBI.R214.01] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request*, it shall issue a challenge to SYNC with cryptographic nonce and salt (*BackupIgnition_Rsp* with *RspCode = 0x01 = Issue Challenge, RspStatus = 0x00 = Reserved, Byte 6 = 0x00, Challenge Nonce = Challenge Nonce, Salt = Salt, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R215.01] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request*, it shall compute, using the cryptographic nonce, another hash of all stored password hashes.

[LBI.R216.01] SYNC shall compute a hash of entered password using received salt and then compute a hash of this result using received nonce.

[LBI.R217.01] SYNC shall respond to the challenge from the BLEM (*BackupIgnition_Rsp* with *RspCode = 0x01 = Issue Challenge*) with computed password hash (*BackupIgnition_Rq* with *OpCode = 0x0C = Reset Challenge Response, KeyIndex = KeyIndex, Password = Challenge Password, KeypadCode = EOS*).

[LBI.R218.01] When the BLEM receives a challenge hash and key index from SYNC (*BackupIgnition_Rq* with *OpCode = 0x0C = Reset Challenge Response, KeyIndex = KeyIndex, Password =*

Challenge Password, KeypadCode = EOS), it shall compare the challenge hash with the password hash associated with the received key index.

[LBI.R219.02] If the BLEM determines that the received password is invalid i.e. challenge hash does not match password hash associated with received key index, it shall increment invalid password counter and then notify SYNC (*BackupIgnition_Rsp with RspCode = 0x0C = Reset Challenge Response Acknowledge, RspStatus = 0x10 = Invalid Password, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R220.02] When SYNC receives an invalid password notification (*BackupIgnition_Rsp with RspCode = 0x0C = Reset Challenge Response Acknowledge, RspStatus = 0x10 = Invalid Password*), the SYNC HMI shall notify the user that the entered password is invalid and provide an option to retry.

[LBI.R221.01] If the BLEM determines that the received password is valid i.e. challenge hash matches password hash associated with received key index, the SYNC HMI shall display the backup password creation screen.

Reset Option 2 starts here, and Reset Option 1 continues here.

[LBI.R058.01] The SYNC HMI shall require the user to enter their new backup password twice. If passwords do not match, the SYNC HMI shall notify the user and provide an option to retry.

[LBI.R059.02] SYNC shall check entered password against password requirements in real time. The SYNC HMI shall not allow the user to proceed to the next screen until their password meets the minimum requirements.

[LBI.R060.02] SYNC shall compute a hash of the entered password and send the result to the BLEM with the key index of the selected device, using either:

1. *OpCode = 0x0D = Reset 1 Password Transmit,* if user is following Reset Option 1
2. *OpCode = 0x0E = Reset 2 Password Transmit,* if user is following Reset Option 2

[LBI.R222.01] Upon receiving the password hash and key index, the BLEM shall either:

1. Verify that the PaaK device associated with this key index is still inside the vehicle if *OpCode = 0x0D = Reset 1 Password Transmit*.

2. Verify that the PaaK device associated with this key index AND a key fob are still inside the vehicle if *OpCode = 0x0E = Reset 2 Password Transmit.*

Note: See details of BCM Interior Registry search in Section 3.1.4

[LBI.R223.01] In Reset Option 1, if the BLEM determines that the PaaK device associated with the received key index is no longer inside the vehicle, then it shall notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x0D = Reset 1 Password Response, RspStatus = 0x07 = PaaK No Longer Detected, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R224.01] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x0D = Reset 1 Password Response, RspStatus = 0x07 = PaaK No Longer Detected*, the SYNC HMI shall display error message that lists phone as missing with options to retry (restart the process) or cancel.

[LBI.R225.01] In Reset Option 2, the BLEM shall respond to SYNC with *BackupIgnition_Rsp* with *RspCode = 0x0E = Reset 2 Password Response* and either:

1. *RspStatus = 0x08 = Fob No Longer Detected* if:
    - The BCM does not detect a key fob in the vehicle (*FobCtlType_D_Stat = 0x1 = Invalid*) AND
    - The BLEM detects the PaaK device associated with the received key index.
2. *RspStatus = 0x07 = PaaK No Longer Detected* if:
    - The BCM detects a key fob in the vehicle (*FobCtlType_D_Stat = 0x2 = Valid*) AND
    - The BLEM does not detect the PaaK device associated with the received key index
3. *RspStatus = 0x09 = PaaK and Fob No Longer Detected* if:
    - The BCM does not detect a key fob in the vehicle (*FobCtlType_D_Stat = 0x1 = Invalid*) AND
    - The BLEM does not detect the PaaK device associated with the received key index

[LBI.R226.01] In Reset Option 2, when SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x0E = Reset 2 Password Response*, the SYNC HMI shall display either:

1. Error message that lists key fob as missing with options to retry (restart the process) or cancel, if:
    - *RspStatus = 0x08 = Fob No Longer Detected* AND
    - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*
2. Error message that lists phone as missing with options to retry (restart the process) or cancel, if:

- *RspStatus = 0x07 = PaaK No Longer Detected* AND
- *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*

3. Error message that lists key fob and phone as missing with options to retry (restart the process) or cancel, if:
   - *RspStatus = 0x09 = PaaK and Fob No Longer Detected* AND
   - *Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*

[LBI.R061.02] The BLEM shall verify that the entered password is not already being used if:

1. In Reset Option 1, the BLEM determines that the PaaK device associated with the received key index is still inside the vehicle.
2. In Reset Option 2, the BLEM determines that the PaaK device associated with the received key index AND a key fob are still inside the vehicle.

[LBI.R227.01] If the BLEM determines that the password is already being used, the BLEM shall notify SYNC of this (*BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0A = Password Already Used, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R228.01] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0A = Password Already Used,* the SYNC HMI shall display a message that password is already being used and instruct user to enter a different password.

[LBI.R062.03] If the entered password is not already being used, the BLEM shall then determine whether there is a keypad code associated with the received key index.

If there is an associated keypad code, the BLEM shall initiate keypad code deletion by responding (with *PaaKCtlActvData_No_Actl*) to periodic RKE challenge from the BCM (*PaaKTrgtActvData_No_Rq*) and sending a request to the BCM to enter keypad programming mode (*KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode*).

Note: See details of BLEM-BCM Keypad programming requirements in Section 3.1.5

If there is no associated keypad code, the BLEM shall delete the current password hash associated with the received key index.

[LBI.R063.03] When the BCM receives *KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode* together with valid RKE response data from the BLEM, it shall enter keypad programming mode and notify the BLEM (*KeyPadCodeProg_D_Stat = 0x2 = LearningMode*) within two seconds and continue to provide notification for up to two seconds.

[LBI.R064.02] When the BLEM receives *KeyPadCodeProg_D_Stat = 0x2 = LearningMode*, it shall send to the BCM the received key index (*PaaKCtlActv_No_Actl = [index]*) and a request to delete the personal keypad code (*KeyPadCodeProg_D_Rq = 0x3 = Delete*).

[LBI.R065.02] When the BCM receives the request to delete the personal keypad code (*KeyPadCodeProg_D_Rq = 0x3 = Delete*) together with the key index (*PaaKCtlActv_No_Actl = [index]*), it shall delete the personal keypad code that is associated with the received key index.

[LBI.R230.01] When the BCM deletes a keypad code, it shall notify the BLEM (*KeyPadCodeProg_D_Stat = 0x4 = Delete*) for one second and then exit programming mode (*KeyPadCodeProg_D_Stat = 0x0 = NormalMode*).

[LBI.R066.03] When the BLEM receives confirmation of keypad code deletion (*KeyPadCodeProg_D_Stat = 0x4 = Delete*), it shall delete the current password hash associated with the received key index.

[LBI.R337.01] When the BLEM deletes a backup password hash as part of reset operation, it shall store the new password hash in its HSM and associate it with the received key index.

[LBI.R338.01] When the BLEM cannot delete the backup password hash, it shall notify SYNC (*BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0C = Password Created Failed, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

Note: This requirement applies whether there is a keypad code associated with the received key index or not.

[LBI.R339.01] When SYNC receives deletion failure response (*BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0C = Password Created Failed*), the SYNC HMI shall notify user of unsuccessful password creation.

[LBI.R231.02] When the BLEM stores a new password hash as part of reset operation, it shall report this to the TCU (*LBIAlert_St* with *Event = 0x09 = Backup Password Reset, Source = 0x00, [timestamp], [Key ID]*) in a BLEM SyncP signed packet (Service Type 0x40/Sub-Service 0x0) as defined in Transfer Protocol BLEM SPSS.

Note: *Reference TP BLEM SPSS and LBI SPSS for BLEM SyncPPacket definition and its payload. Key ID here refers to the Key ID of the PaaK device associated with the backup password that is being reset.*

[LBI.R232.01] When the BLEM stores the new password hash, it shall notify SYNC using either:

1. *RspCode = 0x0D = Reset 1 Password Response and RspStatus = 0x0B = Password Created Successfully,* if user is following Reset Option 1
2. *RspCode = 0x0E = Reset 2 Password Response and RspStatus = 0x0B = Password Created Successfully,* if user is following Reset Option 2

[LBI.R233.01] When SYNC receives *BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0B = Password Created Successfully*, the SYNC HMI shall notify the user of successful password reset.

[LBI.R340.01] When the BCM cannot delete a new keypad code, it shall notify the BLEM (*KeyPadCodeProg_D_Stat = 0x5 = ProgrammingFailture*) for one second and then exit programming mode (*KeyPadCodeProg_D_Stat = 0x0 = NormalMode*).

[LBI.R341.01] When the BLEM receives programming failure response (*KeyPadCodeProg_D_Stat = 0x5 = ProgrammingFailure*), it shall not delete the backup password, but shall notify SYNC of failure (*BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0C = Password Created Failed, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R342.01] When SYNC receives programming failure response (*BackupIgnition_Rsp* with *RspCode = 0x0D/E = Reset 1/2 Password Response, RspStatus = 0x0C = Password Created Failed*), the SYNC HMI shall notify user of unsuccessful password reset.

[LBI.R067.02] After resetting the backup password, the SYNC HMI shall present the user with the option to set up a new personal keypad code.

[LBI.R068.02] If the user chooses not to create a personal keypad code, the SYNC HMI shall inform the user that password reset is complete.

[LBI.R069.02] If the user chooses to create a personal keypad code, the SYNC HMI shall display a screen for entering new personal keypad code.

From here, follow keypad code creation process starting with **LBI.R019** ***and interface details of BLEM-BCM Keypad programming requirements described in Section 3.1.5***

[LBI.R343.01] After SYNC notifies user of successful keypad code creation, it shall inform the user that password reset is complete.

2.1.4.2 Use Case

Actors	User
Pre-conditions	Vehicle is in RUN. User is inside vehicle. One associated PaaK device with password is inside the vehicle.
Scenario Description	1. User selects option to Reset Backup Password for Phone-as-a-Key from PaaK Backup Settings in SYNC. 2. SYNC displays message with reset requirements. 3. User continues. 4. SYNC displays alphanumeric password entry screen and instructs user to enter a backup password. 5. User enters password twice according to password requirements. 6. User selects Enter. 7. SYNC displays message that backup password has been changed successfully and instructs user to commit it to memory. SYNC also asks user if they would like to create a personal keypad code. 8. User declines options to create a personal keypad code.
Post-conditions	Notification that backup password has been deleted is sent to user.
List of Exceptions	
Interfaces	APIM BLEM TCU SDN PaaK FI

2.2 Secondary Functions

2.2.1 Deleting all backup passwords via Master or PaaK Reset

2.2.1.1 Requirements

[LBI.R123.01] When the user selects Master or PaaK Reset through SYNC Settings, the SYNC HMI shall inform the user that all PaaK Backup passwords and associated keypad codes will be erased.

[LBI.R277.02] Once the user follows through with a Master or PaaK Reset, the BLEM shall delete all backup password hashes.

[LBI.R278.02] When deleting all backup password hashes, the BLEM shall determine whether there are any keypad codes associated with these password hashes.

If there are any associated keypad codes, the BLEM shall initiate deletion of all PaaK-associated keypad codes by responding (with *PaaKCtlActvData_No_Actl*) to periodic RKE challenge from the BCM (*PaaKTrgtActvData_No_Rq*) and sending a request to the BCM to enter keypad programming mode (*KeyPadCodeProg_D_Rq = 0x1 = ProgrammingMode*).

2.2.2 Deleting backup password via key revoke

2.2.2.1 Requirements

[LBI.R125.02] When the user revokes the CAK for their PaaK device, the mobile app HMI shall inform the user that, if they have created a backup password and keypad code for their device, these will be deleted at the completion of the revoke request.

2.2.3 Transitioning vehicle from non-motive to motive state with backup password

2.2.3.1 Requirements

[LBI.R128.01] User shall be able to transition vehicle from non-motive to motive state using PaaK Backup.

2.2.3.2 Use Case

Actors	User
Pre-conditions	User has previously activated Phone-as-a-Key for their vehicle via Lincoln mobile app. User is logged into Lincoln app on their mobile phone. User's mobile phone and vehicle are BT connected. User has previously created backup password. Vehicle is locked.
Scenario Description	1. User remote starts vehicle via mobile app. 2. Phone becomes disabled (e.g. battery drained) 3. User approaches locked vehicle, cannot enter. 4. User enters valid keypad code. 5. Vehicle unlocks. 6. User opens door and enters vehicle. 7. User presses brake pedal. 8. SYNC displays backup password entry screen. 9. Without being inactive for more than 30 seconds, user enters valid backup password via SYNC. (This includes inputting the password then selecting Enter. Touch events on screen extend inactivity timeout.) 10. SYNC displays "Password accepted. Start vehicle within 20 seconds. " 11. Within 20 seconds, user presses start button while holding brake pedal. 12. Vehicle transitions from non-motive to motive state.
Post-conditions	User is able to drive away vehicle. User is able to charge their PaaK device in vehicle.
List of Exception Use Cases	User does not enter valid password. User is inactive for more than 30 seconds while SYNC displays password entry screen. User does not start vehicle within 20 seconds of successful password entry.
Interfaces	BLEM APIM BCM

2.2.4 Exiting secure idle state with backup password

2.2.4.1 Requirements

[LBI.R129.04] When the BCM is in a secure idle state and the conditions below are true, it shall trigger the backup password entry screen (*IgnPsswrdDsply_B_Rq = 0x1 = Active*):

1. Brake pedal is pressed OR
2. Accelerator pedal is pressed OR
3. Mechanical Shifter button is pressed AND
4. No key fobs or PaaK devices are detected inside the vehicle AND
5. There is a least one backup password created (*IgnPsswrdActv_B_Stat = 0x1 = Active*)

[LBI.R322.03] When SYNC receives *IgnPsswrdDsply_B_Rq = 0x1 = Active* and engine status, *PwPckTq_D_Stat = 0x1 - PwPckOn_TqNotAvailable or 0x0 - PwPckOff_TqNotAvailable* and the status of Enhanced Valet Mode in SYNC is inactive, SYNC shall display either:

1. A backup password entry screen if *IgnPsswrdLckout_B_Stat = 0x0 = Inactive and Vehicle Connectivity is enabled*
2. A lockout popup if *IgnPsswrdLckout_B_Stat = 0x1 = Active and Vehicle Connectivity is enabled*

Note:
PwPckTq_D_Stat = 0x0 - PwPckOff_TqNotAvailable means engine is not running
PwPckTq_D_Stat = 0x1 - PwPckOn_TqNotAvailable means engine is running in NonMotive mode
PwPckTq_D_Stat = 0x2 – StartInprgrss_TqNotAvail means engine is cranking
PwPckTq_D_Stat = 0x3 - PwPckOn_TqAvailable means engine is running in Motive mode

[LBI.R323.02] When the password entry screen is active and *Ignition_Status = 0x4 = Run*, the SYNC HMI shall return to the previous screen after 30 seconds of inactivity. Keyboard button presses on screen and/or additional receptions of *IgnPsswrdDsply_B_Rq = 0x1 = Active* shall reset inactivity timer.

[LBI.R363.01] When the lockout popup expires and *Ignition_Status = 0x1 = Run*, the SYNC HMI shall return to current screen.

[LBI.R364.01] When the user enters a password at the password entry screen, SYNC shall request a challenge from the BLEM (*BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request, Byte 5 = 0x00*).

[LBI.R365.01] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request*, it shall issue a challenge to SYNC with cryptographic nonce and salt (*BackupIgnition_Rsp* with *RspCode = 0x01 = Issue Challenge, RspStatus = 0x00 = Reserved, Byte 6 = 0x00, Challenge Nonce = Challenge Nonce, Salt = Salt, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R366.01] When the BLEM receives *BackupIgnition_Rq* with *OpCode = 0x01 = Challenge Request*, it shall compute, using the cryptographic nonce, another hash of all stored password hashes.

[LBI.R367.01] SYNC shall compute a hash of entered password using received salt and then compute a hash of this result using received nonce.

[LBI.R368.01] SYNC shall respond to the challenge from the BLEM (*BackupIgnition_Rsp* with *RspCode = 0x01 = Issue Challenge*) with computed password hash (*BackupIgnition_Rq* with *OpCode = 0x02 = Challenge Response, KeyIndex = EOS, Password = Challenge Password, KeypadCode = EOS*).

[LBI.R369.01] When the BLEM receives a challenge hash from SYNC (*BackupIgnition_Rq* with *OpCode = 0x02 = Challenge Response, KeyIndex = EOS, Password = Challenge Password, KeypadCode = EOS*), it shall compare it with the hashes that it computed for the stored passwords.

[LBI.R370.01] If the BLEM determines that the received password is invalid i.e. challenge hash does not match a calculated password hash, it shall increment invalid password counter and then notify SYNC (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x10 = Invalid Password, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*).

[LBI.R371.01] When SYNC receives an invalid password notification (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x10 = Invalid Password*), the SYNC HMI shall notify the user that the entered password is invalid and provide an option to retry.

[LBI.R034.03] If the BLEM determines that the received password is valid i.e. challenge hash matches a calculated password hash, it shall notify SYNC of this (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x0F = Valid Password, Byte 6 = 0x00, Challenge Nonce = EOS, Salt = EOS, Valet Password = EOS, KeyIndex = 0x00, PhoneName = EOS*) and start a 21-second authorization period.

[LBI.R324.02] When the BLEM is in a 21-second authorization period while *Ignition_Status = 0x4 = Run*, the BLEM shall respond positively (*PaakCtlType_D_Stat = 0x2 = Valid, PaakCtlIndx1_No_Actl = [Index]*) to BCM Crypto Start searches (*PaakTrgtType_D_Rq = 0x1 = Crypto, PaakTrgtZone_D_Rq = 0x1 = Interior)*, but negatively to Registry or Polling searches. After this period expires, the BLEM shall respond negatively (*PaakCtlType_D_Stat = 0x1 = Invalid*) to BCM Crypto Start searches.

[LBI.R325.04] When SYNC receives a valid notification from the BLEM (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x0F = Valid Password*) and engine status, *PwPckTq_D_Stat = 0x1 - PwPckOn_TqNotAvailable*, the SYNC HMI shall notify the user that the entered password has been accepted and that they can now press the brake and shift out of park in order to drive the vehicle.
This message shall display for 20 seconds unless vehicle engine status *PwPckTq_D_Stat* changes to *PwPckOn_TqAvailable* (engine running and in Motive mode) or *PwPckOff_TqNotAvailable* (engine is not running), then this message shall be dismissed.

[LBI.R383.01] When SYNC receives a valid notification from the BLEM (*BackupIgnition_Rsp with RspCode = 0x02 = Challenge Response Acknowledge, RspStatus = 0x0F = Valid Password*) and engine status, *PwPckTq_D_Stat = 0x0 - PwPckOff_TqNotAvailable*, the SYNC HMI shall notify the user that the entered password has been accepted and that they can now press the brake and start button in order to start the vehicle.
This message shall display for 20 seconds unless the vehicle engine status *PwPckTq_D_Stat* changes to *PwPckOn_TqAvailable* (engine running in Motive mode) or *PwPckOn_TqNotAvailable* (engine is running in NonMotive mode), then this message shall be dismissed.

[LBI.R283.04] When the BCM is in a secure idle state and the conditions below are true, it shall exit the secure idle state:

1. Any door transitions from open to closed OR
2. Brake pedal is pressed OR
3. Accelerator pedal is pressed OR
4. Mechanical Shifter button is pressed OR
5. Seatbelt becomes buckled AND
6. BLEM responds positively to BCM Crypto Start search

The BCM shall suspend secure idle operation until next ignition cycle when the keypad code associated with index 63 is stored in BCM.

[LBI.R284.02] When there exists a keypad code associated with key index 63 in the BCM, secure idle operation shall be suspended until the next key cycle.

Note: This means that when a user activates Enhanced Valet Mode, secure idle will be disabled, even if the vehicle is currently in a secure idle state. This also means that deactivating Enhanced Valet Mode will re-enable secure idle.

2.2.4.2 Use Case

Actors	User
Pre-conditions	User has previously created backup password. Vehicle is in RUN. Vehicle transmission is in park. User is outside and away from vehicle. Vehicle is unlocked. No associated key fobs or phones-as-keys are inside vehicle.
Scenario Description	1. User returns to vehicle. 2. User attempts to start engine/shift vehicle out of park. 3. Cluster displays “No Key Detected”. 4. SYNC displays backup password entry screen. 5. Without being inactive for more than 30 seconds, user enters valid backup password via SYNC. (This includes inputting the password then selecting Enter. Touch events on screen extend inactivity timeout.) 6. SYNC displays “Password accepted” and returns to Home screen. 7. Cluster no longer displays “No Key Detected”.
Post-conditions	User is able to drive away vehicle
List of Exception Use Cases	
Interfaces	APIM BCM BLEM IPC

3 General Requirements

3.1 Functional Requirements

3.1.1 SYNC

Note: In the requirements below "password entry screen" refers to both the backup password entry screen and the valet password entry screen for starting the vehicle.

[LBI.R195.02] If SYNC is running the welcome animation when SYNC receives *IgnPsswrdDsply_B_Rq = 0x1 = Active*, SYNC shall cancel the greeting timer and display the password entry screen after the welcome animation is finished.

[LBI.R196.03] After 30 seconds of inactivity at the password entry screen:

- The SYNC HMI shall go to the previous screen if:
  - *Ignition_Status = 0x4 = Run* OR
  - *Ignition_Status = 0x1 = Off* and *Delay_Accy = 0x1 = On* OR
  - *Ignition_Status = 0x1 = Off* and SYNC is in Extended Play mode.
- SYNC shall suspend if:
  - *Ignition_Status = 0x1 = Off, Delay_Accy = 0x0 = Off,* and SYNC is not in Extended Play mode.

Keyboard button presses on screen and/or additional receptions of *IgnPsswrdDsply_B_Rq = 0x1 = Active* shall reset inactivity timer.

[LBI.R306.02] After the lockout popup expires:

- The SYNC HMI shall go to the previous screen if:
  - *Ignition_Status = 0x4 = Run* OR
  - *Ignition_Status = 0x1 = Off* and *Delay_Accy = 0x1 = On* OR
  - *Ignition_Status = 0x1 = Off* and SYNC is in Extended Play mode.
- SYNC shall suspend if:
  - *Ignition_Status = 0x1 = Off, Delay_Accy = 0x0 = Off, and SYNC is not in Extended Play mode.*

[LBI.R295.02] Once SYNC transmits a password hash to the BLEM, it shall delete this password hash from memory.

[LBI.R296.02] If SYNC has received multiple challenges nonces, it shall recognize only the most recent one as valid.

[LBI.R379.02] When SYNC transmits a keypad code that is associated with a backup password to the BLEM, it shall structure the data as an N_{th} button sequence where each button is represented by three bits.
TP method specification defines the bytes 6-9 of the keypad code when SYNC sends BackupIgnition_Rq with Opcode = 0x08.

The mapping of button to bit value as follows:

000 = NULL
001 = “1/2” button pressed
010 = “3/4” button pressed
011 = “5/6” button pressed
100 = “7/8” button pressed
101 = “9/0” button pressed

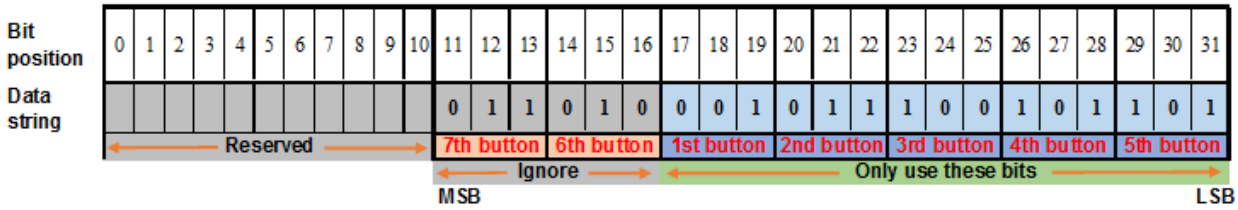
When a customer is creating a keypad code, the SYNC shall provide an appropriate screen (based on vehicle configuration) with either 7-digit or 5-digit codes.
Prior to transmitting a keypad code data to the BLEM, the SYNC shall verify the vehicle configuration (e.g. there are markets that require the use of 7-digit codes and 5-digit codes), and then send bit string data.
If the SYNC detects a misconfiguration (for example, if configuration calls for 7-digit codes but the bit string data consists of 5-digit codes), it shall set a Control Module Configuration Incompatible DTC and not transmit a keypad code data to the BLEM.
Instead, it shall provide a warning/notification pop up to a customer via HMI interface to indicate an error has occurred and instruct a user to take a vehicle for service.

Note: *SYNC data shall always be represented with 7-digit codes (e.g. 7-button press sequence). When 5-digit codes are implemented, the Sixth and Seventh button press parameters shall be set to Null.*

For example, a keypad code of 1234567 consists of keypad buttons **“1/2”, “1/2”, “3/4”, “3/4”, “5/6”, “5/6”, “7/8”.**

As a bit string, this is represented as 0000 0000 000 **$100_{\text{seventh button}}$ $011_{\text{sixth button}}$ $001_{\text{first button}}$ $001_{\text{second button}}$ $010_{\text{third button}}$ $010_{\text{forth button}}$ $011_{\text{fifth button}}$**

Here is another example of bit string data for keypad code **1579936** as sent out by SYNC and received by BLEM:



[LBI.R409.01] When a customer is creating a personal keypad code, the SYNC shall verify customer acceptable codes based on the vehicle configuration (e.g. there are markets that require the use of 7-digit codes and 5-digit codes).
If SYNC determines the configuration is for 7-digit codes, then it shall apply the following restrictions:

- Desired door keypad code cannot consist of all the same numbers
  - customer presses button **"1/2"** seven (7) times
  - customer presses button **"3/4"** seven (7) times
  - customer presses button **"5/6"** seven (7) times
  - customer presses button **"7/8"** seven (7) times
  - customer presses button **"9/0"** seven (7) times

When a single button has been pressed six (6) consecutive times, that button shall become grey out for the last digit entry and SYNC screen shall also be populated with instruction stating "Desired 7-digit keypad code must not consist of selecting the same button seven times"

3.2 HMI Requirements

[LBI.R297.01] Any time SYNC displays a list of PaaK devices, the list shall be sorted by key index, with the lowest index at the top.

3.2.1 PaaK Backup Settings

[LBI.R130.01] SYNC shall provide a menu for PaaK Backup settings when the vehicle is configured for Phone-as-a-Key:

DE05	1	3	Phone as a Key	0	0 – Not Present 1 – Present	N/A

[LBI.R131.03] The PaaK Backup settings menu shall provide buttons for the following functions:

- Create backup passwords/keypad codes for phones-as-keys
- Reset backup passwords/keypad codes for phones-as-keys
- Delete backup passwords/keypad codes for phones-as-keys

[LBI.R132.03] SYNC shall not allow the user to initiate password creation, deletion, or reset from the HMI unless the ignition is in Run (*Ignition_Status = 0x4 = Run*) and transmission is in Park (*GearLvlPos_D_Actl = 0x0 = Park*). The buttons to initiate these functions shall be greyed out unless these conditions are met.

[LBI.R373.01] If password creation, deletion, or reset are active in SYNC (e.g. user is in the process of creating a backup password), and the ignition changes from Run or the transmission changes from Park, then SYNC shall display a message with driving restriction information, exit the function and return to the PaaK Backup settings menu.

3.3 Security Requirements

[LBI.R138.01] Passwords shall never be transmitted across any interface in clear-text.

3.3.1 Password Storage

[LBI.R140.01] The BLEM shall securely store within HSM all customer passwords created and used to enable vehicle start and drive-away.

[LBI.R141.01] Passwords shall never be stored in the clear, but instead shall be stored in a salted and hashed format, defined as:

$$Programmed\ Hash = SHA256(Salt + Password)$$

Note that the output of SHA256 will always be a 256-bit (32-byte) hash – thus storage requirements are consistent regardless of password length.

3.3.2 Backup Passwords

3.3.2.1 Programming

[LBI.R143.01] The BLEM shall not accept any new backup passwords for LBI unless all of the following conditions have been met:

- The customer has opted-in to using the feature
- At least one PaaK device authorized and enabled for the given vehicle (i.e. with a provisioned CAK) is inside the vehicle and is in session (see BLE Interface Security Specification)
- A password does not already exist for the given PaaK device/vehicle pairing
- At least one PEPS key fob is detected inside the vehicle

[LBI.R144.02] PaaK device checks and key fob checks shall be executed when the BLEM has received a password hash to be stored.

This mitigates potential time of check/time of use vulnerabilities.

[LBI.R145.01] All backup passwords MUST be associated internally on the BLEM to a CAK authorized for the given vehicle.

[LBI.R146.03] For CGEA1.3C architecture with SYNC 3/ or Feature Bundle 4 (FB4) vehicle programs the **passwords shall be a minimum of 5 characters** in length if a mixture of letters, numbers, and symbols are used.
For FNV2 architecture with SYNC 4/ or Feature Bundle 5 (FB5) vehicle programs the **passwords shall be a minimum of 6 characters** in length if a mixture of letters, numbers, and symbols are used.
For CGEA1.3C architecture with SYNC 3/ or Feature Bundle 4 (FB4) vehicle programs the **passwords shall be a minimum of 8 characters** in length if only numbers are used (for example, Enhanced Valet passcode).
For FNV2 architecture with SYNC 4/ or Feature Bundle 5 (FB5) vehicle programs for European market, the **passwords shall be a minimum of 10 characters** in length if only numbers are used (for example, Enhanced Valet Passcode).

[LBI.R147.01] Passwords shall be a maximum of 64 characters in length.

[LBI.R148.01] Backup passwords shall not be directly displayed on any HMI.

[LBI.R149.01] An indicator shall be displayed on the HMI indicating the relative strength of the user's selected password.

[LBI.R150.02] The strength indicator shall have four levels of strengths: weak, fair, good, and strong. These levels shall be indicated using a four-segment fill bar. If minimum requirements are not met, bar shall be empty. If password is weak, bar shall fill ¼ with red color. If password is fair, bar shall fill ½ with orange color. If password is good, bar shall fill ¾ with yellow color. If password is strong, bar shall fill completely with green color.

[LBI.R178.02] The following rules shall be used to determine back up password strength:

1. Weak: Password must have at least ten (10) characters if password consists only of numbers or at least six (6) characters if password does not consist only of numbers.

2. Fair: Password must have at least ten (10) characters including at least one (1) lower-case letter, one (1) upper-case letter, and one (1) number.

3. Good: Password must have at least twelve (12) characters including three of the following four types of characters: lower-case letter, upper-case letter, number, special character (including space). Password also must have no more than two identical characters in a row

4. Strong: Password must have at least fourteen (14) characters including three of the following four types of characters: lower-case letter, upper-case letter, number, special character (including space). Password also must have no more than two identical characters in a row.

~~1. Weak: Password must have at least eight (8) characters if password consists only of numbers or at least five (5) characters if password does not consist only of numbers.~~

~~2. Fair: Password must have at least eight (8) characters including at least one (1) lower-case letter, one (1) upper-case letter, and one (1) number.~~

~~3. Good: Password must have at least ten (10) characters including three of the following four types of characters: lower-case letter, upper-case letter, number, special character (including space). Password also must have not more than two identical characters in a row.~~

~~4. Strong: Password must have at least twelve (12) characters including three of the following four types of characters: lower-case letter, upper-case letter, number, special character (including space). Password also must have not more than two identical characters in a row.~~

- The SYNC shall utilize password strength controls according to the following security guidelines:

https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

- The SYNC must use at the minimum 10K common password list and if the password is found in that list the ranking shall be marked not higher than “fair”:

https://github.com/danielmiessler/SecLists/blob/master/Passwords/xato-net-10-million-passwords-10000.txt

- A password that does contain two (2) or more similar letters/numbers shall be excluded from the “strong” or “good” ranking.
- A password that does not contain two (2) or more similar letters/numbers shall be eligible for the “strong” or “good” ranking.

For the following requirements describing hash calculation, the ‘+’ operand is construed to mean concatenation, not addition.

[LBI.R151.02] Backup passwords shall be transmitted from the in-vehicle HMI in a salted and hashed format (“Programmed Hash”), using the following mechanism:

$$Programmed\ Hash = SHA256(Salt + Password)$$

Note: *the "+" operator in above calculations means append, not add. The salt and nonce values must be a lower case hex bytes. There is no space between (salt and password) string, it is one string of hex values. SYNC must convert the password that user is trying to create from asci value into hex string before proceeding with Programmed Hash calculation.*

Calculation Example

Programmed hash = SHA256(e7e272cf7bbf00ab9874ad03bde24626717765313233) = 35effe7d0c505913286470ba328f835da9067cd1c9ca2817102db7ec6f95b4c8

Where

Salt = e7e272cf7bbf00ab9874ad03bde24626

Desired password = qwe123 → converted to hex = 717765313233

[LBI.R152.01] If more than one PaaK device is discovered within the vehicle without an associated backup password, the user shall be prompted to select a device to associate the password with.

3.3.2.2 Deletion

[LBI.R153.01] Customers shall be required to enter the backup password to delete it via the in vehicle HMI.

[LBI.R154.01] If a CAK is revoked for any reason and a backup password is associated to that CAK, the backup password shall immediately be deleted and not allowed for further usage.

[LBI.R155.01] Backup passwords shall only be deleted if the vehicle is in a motive mode (i.e. an authentication step has been performed enabling the user to start the vehicle, either by PaaK device, key fob or backup password).

3.3.3 Password Usage

Note: the procedure described below applies for both temporary and backup passwords.

[LBI.R156.01] A challenge/response mechanism shall be used with the password hash to authenticate and start the vehicle via the in-vehicle HMI.

[LBI.R157.01] On request, the BLEM shall generate a random 256-bit nonce using the best available RNG. If possible, a true RNG shall be used. This nonce shall be sent to the in-vehicle HMI module.

[LBI.R158.02] When the user enters a password, the in-vehicle HMI module shall perform two rounds of hashing before transmitting the response to the BLEM. The first shall calculate the Programmed Hash:

$$Programmed\ Hash = SHA256(Salt + Backup\ Password)$$

Note: *see notes for LBI.R151.02*

[LBI.R159.02] Once the Programmed Hash has been calculated, the in-vehicle HMI module shall then calculate and transmit the "Authentication Hash", using the following mechanism:

$$Authentication\ Hash = SHA256(Nonce + Programmed\ Hash)$$

Note: *the "+" operator in above calculations means append, not add. The nonce value must be a lower case hex byte. There is no space between (nonce and programmed hash) string, it is one string of hex values.*

Calculation Example

Authentication hash = SHA256(fb03845b994809d8b265aba4a7c7c64235d125151d7f1eb3fcf42252148a483435effe7d0c505913286470ba328f835da9067cd1c9ca2817102db7ec6f95b4c8) = **7a86e7379848b4106150e3674aaf0f99a1b408588d8b402742782e6db0d16c3e**

Where

Nonce = fb03845b994809d8b265aba4a7c7c64235d125151d7f1eb3fcf42252148a4834

Programmed Hash = 35effe7d0c505913286470ba328f835da9067cd1c9ca2817102db7ec6f95b4c8

Refer to APIM / BLEM TP specs (BackupIgnition_Rq and BackupIgnition_Rsp) for more details on where to apply Programmed hash and where to apply Authentication hash.

BLEM and Sync both shall validate the output of Programmed hash or Authentication hash depending upon which opcode they are comparing.

[LBI.R160.01] Upon sending the nonce to the in-vehicle HMI module, the BLEM shall also calculate the Authentication Hash for all stored passwords.

This is done because the BLEM does not know ahead of time which password to expect, and thus it must compare the received value to all known passwords to find a match.

[LBI.R161.01] Upon receiving the Authentication Hash, the BLEM shall compare the received values to its calculated Authentication Hashes. A constant time algorithm shall be used when comparing the hashes. If a match is found, the system shall indicate success to the user and allow vehicle start. If a match is not found, a failure should be reported to the user.

[LBI.R162.01] If the user does not provide a valid password within 5 attempts, the system shall lock out further attempts for 5 minutes. The authenticating system (the BLEM) shall be the master of this logic.

[LBI.R163.01] After the first 5-minute lockout, the user shall be permitted 5 additional attempts to enter a valid password. If the user does not enter a valid password within these 5 attempts, the system shall lock out further attempts for another 5 minutes. This lockout process shall repeat indefinitely.