Functions	Precondiction	Steps to process	At service	At characteristic	Package from phone	Return from device	Notes
Add device	Phone have not bonded	Connect to device	by BLE protocol	by BLE protocol	by BLE protocol	by BLE protocol	
		Discover services	by BLE protocol	by BLE protocol	by BLE protocol	by BLE protocol	
		Enable Auth notification	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050021-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Write Auth data over characteristic	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050021-0a2c-eeac-f448-7b1e8856cdd0	PITECH_CIPHER(SHA256(PIN_CODE) + USER_ID)	by BLE protocol	PIN_CODE: 4 bytes, USERID: 12 bytes, PITECH_CIPHER: have not decided
		Receive result from device	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050021-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: success; 0x02; fail	
		Receive 32 bytes of device's public key	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050021-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	32 bytes of device's public key	This is 2 steps to create a COMMON_KEY(32 bytes) that bases on the ECDH cryption
		Send 32 bytes of phone's public key	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050021-0a2c-eeac-f448-7b1e8856cdd0	32 bytes of phone's public key	by BLE protocol	
		Create bonding request	by BLE protocol	by BLE protocol	by BLE protocol	by BLE protocol	
		Enable Sampling notification	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050013-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Enable Unlock notification	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050011-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Enable Locating notification	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050012-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Enable OBDII notification	6d050030-0a2c-eeac-f448-7b1e8856cdd0	6d050031-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Write Sampling data over characteristic	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050013-0a2c-eeac-f448-7b1e8856cdd0	0x01	by BLE protocol	
		Pop up " Mở núm khóa để hoàn tất'	null	null	null	null	
		Receive data	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050013-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: success; 0x02: fail	
Unlock bike	Connected and Bonded to device	Write Unlock data over characteristic	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050011-0a2c-eeac-f448-7b1e8856cdd0	0x01	by BLE protocol	
	Enabled unlock notification	Receive data	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050011-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: success; 0x02: fail,0x03: limited by the range, 0x04: able to unlocked by key fob, 0x05: has already unlocked, 0x06: has already got UNLOCK command, 0x07: have no sample, 0x08: remind close the lock	
Locating bike	Connected and Bonded to device	Write Locating data over characteristic	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050012-0a2c-eeac-f448-7b1e8856cdd0	0x01	by BLE protocol	
	Enabled locating notification	Receive data	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050012-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: success; 0x02: fail	
OBDII	Connected and Bonded to device Enabled OBDII notification	Receive data	6d050030-0a2c-eeac-f448-7b1e8856cdd0	6d050031-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	speed = data[3],RPM = data[4]x100 + data[5], battery = data[6]/10, engine_state = data[7], side_stand = data[8]	The received packet from device consist of 9 bytes, the 3 fisrt bytes will be defined after, the 4th byte is speed of bike, the 5th byte multiple of 100 and plus 6th byte is rotation speed of engine, the 7th byte divide by 10 is battery, the 8th byte is state of engine (ON/OFF), the 9th byte is state of side stand (ON/OFF)
Create Sharing	Only owner is created sharing	Encrypt data	null	null	AES256CBC(USED_TIME + COUNTER + SHA256(PIN_CODE + GUEST_ID) + PADDING, COMMON_KEY)	null	A packet consist of 48 bytes (must be a multiple of 16 bytes). The packet is encrypted by AES256CBC using COMMON_KEY; USED_TIME consist of 4 bytes, the fisrt byte to detect type of sharing, the next 3 bytes is UNIX time that is used time by guest; COUNTER is 2 bytes of number to difference between sharing times, to prevent reuse packet, COUNTER will be decreased after sharing time; SHA256(PIN_CODE + GUEST_ID) consist of 32 bytes.
		Send sharing data	null	null		null	
Get Sharing	Shared guest; Phone have not bonded yet	Get sharing data	null	null	null	null	
		Connect to device	by BLE protocol	by BLE protocol	by BLE protocol	by BLE protocol	
		Discover services	by BLE protocol	by BLE protocol	by BLE protocol	by BLE protocol	
		Enable sharing notification	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Write sharing data over characteristic	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	AES256CBC(USED_TIME + COUNTER + SHA256(PIN_CODE + GUEST_ID), COMMON_KEY)	by BLE protocol	
		Receive a GUEST_ID request	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x03: GUEST_ID request	
		Send GUEST_ID	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	PITECH_CIPHER(GUEST_ID + SALT)	by BLE protocol	
		Receive data	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: accept; 0x02: deny	
		Create bonding request	by BLE protocol	by BLE protocol	by BLE protocol	by BLE protocol	
Delete Sharing	Only owner is deleted sharing	Enable sharing notification	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Write changing data over characteristic	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	PITECH_CIPHER(SHA256(PIN_CODE + GUEST_ID) + COUNTER)	by BLE protocol	
	Connected and Bonded to device	Receive data	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050022-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol		
Change PIN_CODE	Only owner is changed PIN_CODE	Enable change PIN_CODE notification	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050023-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Write changing data over characteristic	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050023-0a2c-eeac-f448-7b1e8856cdd0	PITECH_CIPHER(SHA256(CURRENT_PIN_CODE) + NEW_PIN_CODE)	by BLE protocol	
	Connected and Bonded to device	Receive data	6d050020-0a2c-eeac-f448-7b1e8856cdd0	6d050023-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: success; 0x02: fail	
Update firmware OTA trigger	Only owner is triggered the update OTA	Enable DFU notification	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050014-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	by BLE protocol	
		Write changing data over characteristic	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050014-0a2c-eeac-f448-7b1e8856cdd0	0x01	by BLE protocol	
	Connected and Bonded to device	Receive data	6d050010-0a2c-eeac-f448-7b1e8856cdd0	6d050014-0a2c-eeac-f448-7b1e8856cdd0	by BLE protocol	0x01: success; 0x02: fail	