

2018

[LOCK SERVER API SPEC]

This document is a specification for the LOCK SERVER API, which provides APIs for Lock Server interaction and basic management for locks and keys.

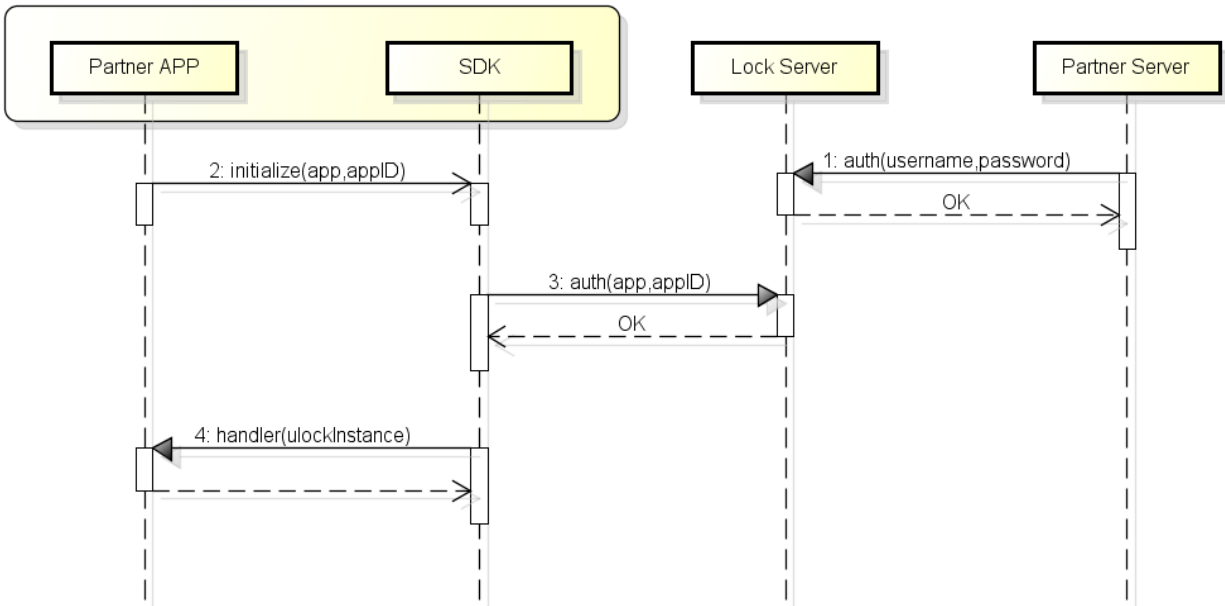
Catalog

1 Use Cases	2
1.1 Authentication.....	2
1.2 Activate Locks	3
1.3 Lock / Unlock.....	4
1.4 Reset Locks.....	6
1.5 Share Keys by Partner Server	7
1.6 Share Keys by Other System.....	8
2 APIs.....	9
2.1 Authentication.....	9
2.1.1 Authentication of Server Account	9
2.1.2 Refresh Access Token	10
2.2 Lock Basic Operations.....	11
2.2.1 Retrieve All Locks	11
2.2.2 Retrieve Admin Key	12
2.2.3 Retrieve Permanent Key	13
2.2.4 Retrieve Guest Key	14
2.3 Gateway Operations.....	16
2.3.1 Retrieve All Gateways	16
2.3.2 Retrieve Gateway Status.....	16
2.4 Lock Remote Operations	17
2.4.1 Retrieve Lock Status	17
2.4.2 Setup Guest Password.....	18
2.4.3 Cancel Guest Password.....	20
2.4.4 Remote Unlock	21
2.4.5 Retrieve Instruction Status	22
2.5 Other Operations	23
2.5.1 Create Lock Keeper Account.....	23
2.5.2 Guest Key Sharing Callback	24

1 Use Cases

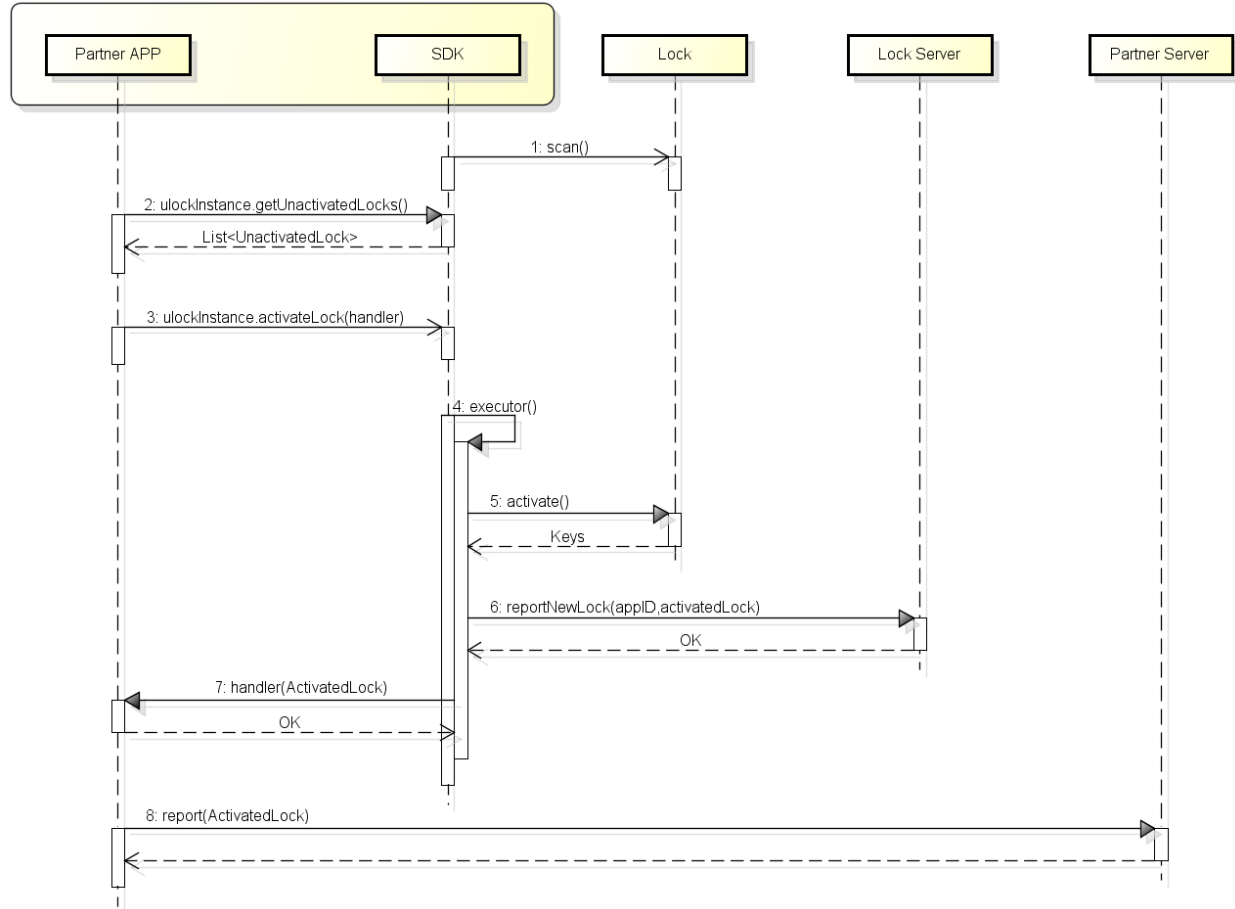
For use cases involving SDK APIs, please refer to *Lock SDK Specification*.

1.1 Authentication



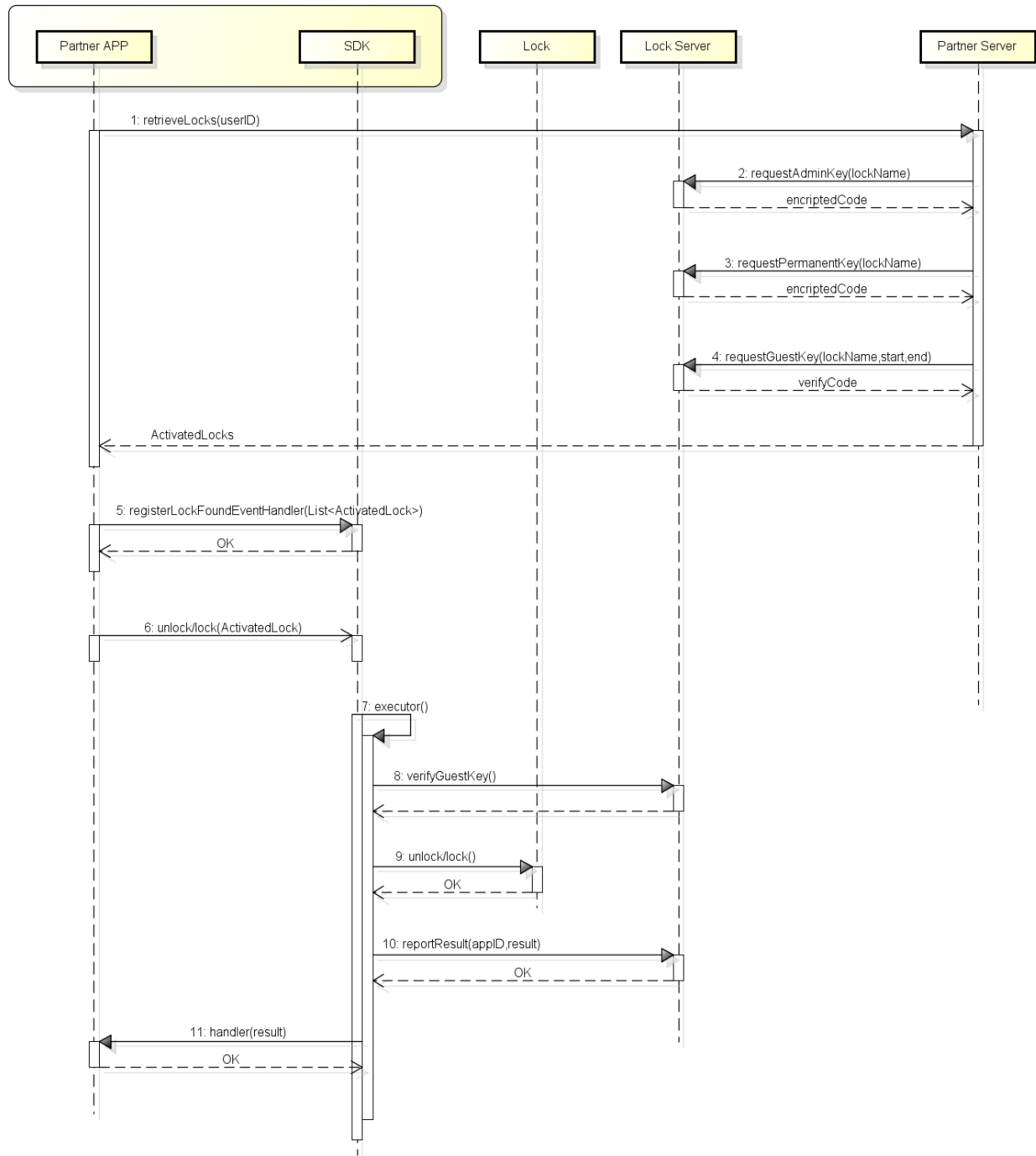
1. Partner Server sends authentication request to Lock Server
2. Partner APP initializes SDK (asynchronous)
3. SDK sends authentication request to Lock Server with appId when initializing
4. SDK calls the callback when authenticated, and return an initialized instance of ULockAPI

1.2 Activate Locks



1. SDK scans for unactivated locks after initialization
2. Partner APP gets unactivated lock list with SDK API
3. Partner APP uses SDK API to activate the lock (asynchronous)
4. SDK executes the activate task
5. SDK activates the lock, and gets keys from the activated lock
6. SDK reports the activated lock to Lock Server with appID
7. SDK calls the handler and returns an ActivatedLock instance after it was reported
8. Partner APP reports the activated lock to Partner Server

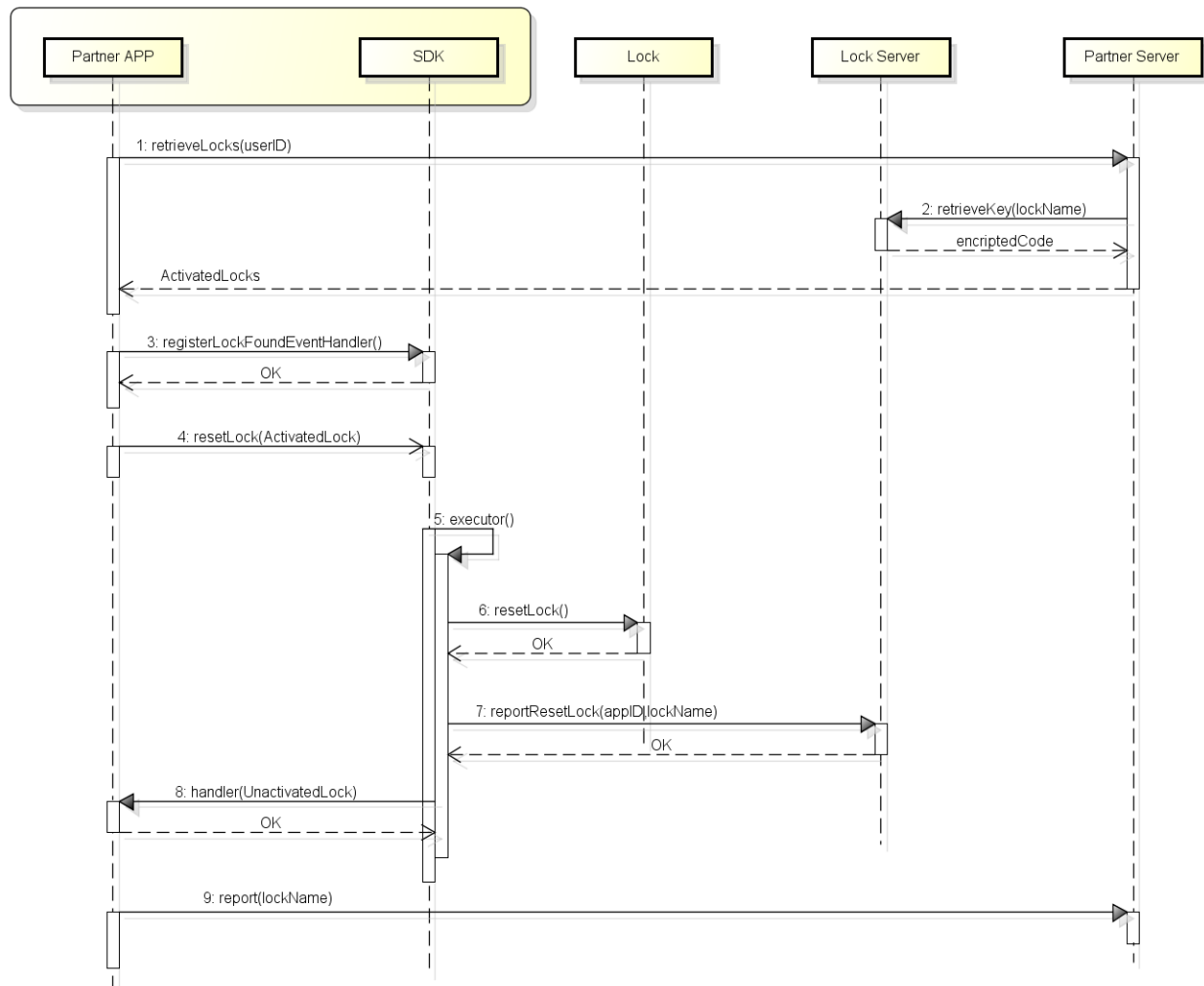
1.3 Lock / Unlock



1. Partner APP sends request to Partner Server for user's lock list
2. For admin key, Partner Server sends request to Lock Server for admin key
Skip this step if the admin key has been cached locally
3. For permanent key, Partner Server sends request to Lock Server for permanent key
Skip this step if the permanent key has been cached locally

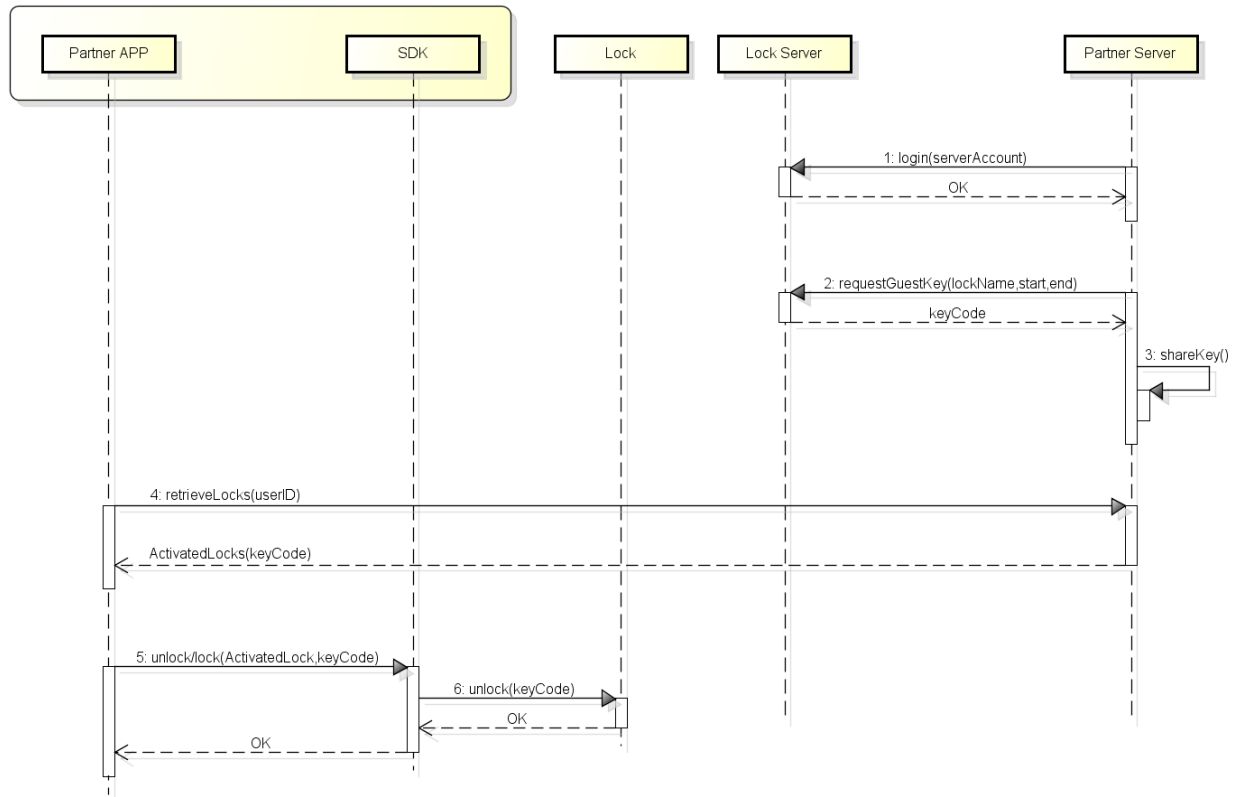
4. For guest key, Partner Server sends request to Lock Server for guest key
Skip this step if the guest key has been cached locally
Then Partner Server returns lock list to Partner APP
5. Partner APP uses SDK API to start listeners for handling locks
6. Partner APP use SDK API to lock/unlock the device (asynchronous)
7. SDK executes the lock/unlock task
8. If using guest key to lock/unlock, SDK sends request to Lock Server for key verification
9. SDK sends lock/unlock commands to the device, and gets response
10. SDK reports the lock/unlock result to Lock Server with appID
11. SDK calls the handler and returns lock/unlock result after it was reported

1.4 Reset Locks



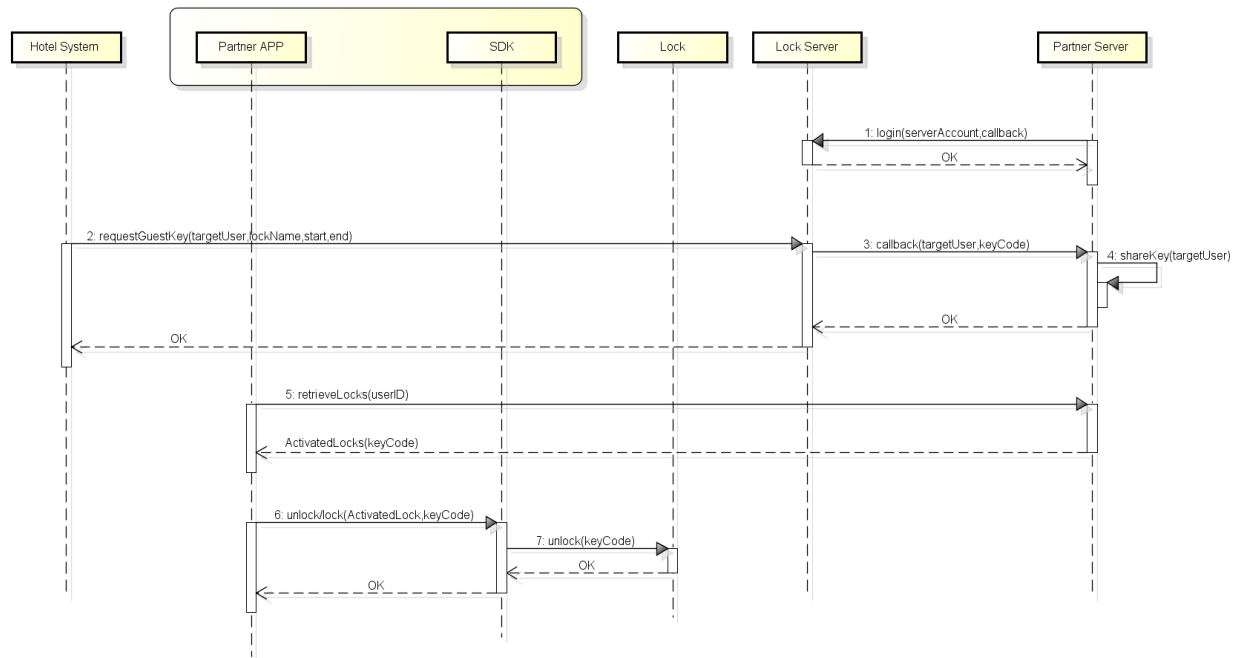
1. Partner APP sends request to Partner Server for user's lock list
2. Partner Server sends request to Lock Server for lock keys; Lock Server returns encrypted keys; Partner Server returns lock list to Partner APP
3. Partner APP uses SDK API to start listeners for handling locks
4. Partner APP uses SDK API to reset the lock (asynchronous)
5. SDK executes the reset task
6. SDK sends reset commands to the device, and gets response
7. SDK reports the reset lock to Lock Server with appID
8. SDK calls the handler and return an UnactivatedLock instance after it was reported
9. Partner APP reports the reset lock to Partner Server

1.5 Share Keys by Partner Server



1. Partner Server succeeds to login Lock Server with serverAccount
2. Partner Server sends request to Lock Server for a guest key with specified start time and end time; Lock Server returns key (encrypted code)
3. Partner Server shares the key to target user
4. Target user uses Partner APP to retrieve the shared key
5. Target user uses Partner APP to unlock the lock with the shared key
6. SDK succeeds to unlock

1.6 Share Keys by Other System



1. Partner Server succeeds to login Lock Server with serverAccount and callback
2. Hotel System or other system sends request to Lock Server for a guest key with specified start time, end time and target user
3. Lock Server call the callback of Partner Server, with parameters of target user, start time, end time and key (encrypted code)
4. Partner Server shares the key to target user
5. Target user uses Partner APP to retrieve the shared key
6. Target user uses Partner APP to unlock the lock with the shared key
7. SDK succeeds to unlock

2 APIs

Lock Server provides restful APIs for Partner Server. Please use **Query String** for Get requests; use **JSON String** in HTTP body for Put/Post request, and set Headers with "**Content-Type**": "**application/json**" at the same time. Lock Server APIs are **UTF-8** character encoding.

Developers can test all APIs at *Lock Server Test Environment* by replacing **server.ip** in URL with 121.40.42.36. User/password for the test environment is [testserver/123456](#). Please refer to examples of each API for detail.

2.1 Authentication

2.1.1 Authentication of Server Account

Partner Server uses this API to login Lock Server.

Request URL	https://server.ip/locks/api/apps/v1/servers/accesstoken		
Request Method	POST		
Header	Value	Note	
Content-type	application/json		
Parameters	Required	Note	
username	Y	ID of Partner Server	
password	Y	Password of Partner Server	
device_mac	Y	Device Token of Partner Server	
callback_address	N	Address of callback, refer to session 2.5.2 for detail	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
access_token	string	Y	Access token
refresh_token	string	Y	Refresh token
accessToken_expires	long	Y	Effective time length of access token (millisecond)
refreshToken_expires	long	Y	Effective time length of refresh token (millisecond)

Example:

POST https://121.40.42.36/ilocks/api/apps/v1/servers/accesstoken

Request:

```
{
  "password": "123456",
  "device_mac": "Server",
  "username": "testserver",
  "callback_address": "10.10.10.10:8080"
}
```

Response:

```
{
  "ack": 0,
  "msg": "succeed",
  "access_token": "504526a9128055b25b6fae97c7a22e4927c9f425b3856bf8",
  "refresh_token": "4d9b5a1415904a36abc5c8979d32e526a97c3d4e5da983c1",
  "accessToken_expires": 10800000,
  "refreshToken_expires": 604800000
}
```

2.1.2 Refresh Access Token

Partner Server uses this API to refresh access token.

Request URL	https://server.ip/ilocks/api/apps/v1/servers/accesstoken		
Request Method	PUT		
Header	Value	Note	
Content-type	application/json		
Parameters	Required	Note	
refresh_token	Y	Refresh token	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
access_token	string	Y	Access token
refresh_token	string	Y	Refresh token
accessToken_expires	long	Y	Effective time length of access token (millisecond)

refreshToken_expires	long	Y	Effective time length of refresh token (millisecond)
----------------------	------	---	--

Example:

None.

2.2 Lock Basic Operations

Developers should use the APP armed with Lock SDK to activate and report the lock before doing any other lock operations (refer to *Lock SDK Specification* for detail). If not planning to develop a new APP with Lock SDK, developers can use the existing *ULockSDKDemo* APP to activate the lock instead.

Notice: locks activated by *ULockSDKDemo* APP are only available in test environment. You can download *ULockSDKDemo* APP at <http://121.40.42.36/ULock-SDKDemo/download.html>, or scan the QR code below:



2.2.1 Retrieve All Locks

Partner Server uses this API to get all locks' basic information, which is required for later operations, i.e. retrieving keys.

Request URL	https://server.ip/ilocks/api/apps/v1/locks	
Request Method	GET	
Header	Value	Note
Authorization	bearer <access-token>	<access-token> is returned by

		authentication	
Content-type	application/json		
Parameters	Required	Note	
none	N		
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	JSON Array	Y	information
-- s_lock_name	string	Y	Lock name

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/locks

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":[
    {"s_lock_name":"XXXXXX"},
    {"s_lock_name":"XXXXXX"}
  ]
}
```

2.2.2 Retrieve Admin Key

Partner Server uses this API to get admin keys of specified lock. Admin keys can be used to lock/unlock/reset the lock device, and have no time limits.

Request URL	https://server.ip/ilocks/api/apps/v1/locks/:lockname/adminKey		
Request Method	GET		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	

none	N	Parameter lockname has been specified in URL.	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	information
-- s_key_code	String	Y	encrypted admin key

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/locks/MJ000006/adminKey

Request:

none

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "s_key_code":"47d8d60a474be711e2feb090bd266f614f50086433c383c7bb60ee29deb8c9992dec4606a6ae4f2535a69fd9b726a89673405799d473bf745d5c1e98ad0ffa0aa7e2cef9702247192d4291f533786c816df5f836b09865caa6bd2ad9f5889a9bd0dc4669d2c163264ed772ad8fd9c275889e0328b2dce1a685430e7e9b3467e5e0c37da298bbe3261aa9eeb5551f7ae1de0bc0a74f4a99c474baaa38d73d36a92ca253e676139e9ecda63e35d2212dd2"
  }
}
```

2.2.3 Retrieve Permanent Key

Partner Server uses this API to get permanent keys of specified lock. Permanent keys can be used to lock/unlock the lock device, have no time limits, but not able for reset operation.

Request URL	https://server.ip/ilocks/api/apps/v1/locks/:lockname/permanentKey		
Request Method	GET		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		

Parameters	Required	Note	
none	N	Parameter lockname has been specified in URL.	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	information
-- s_key_code	String	Y	encrypted permanent key

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/locks/MJ000006/permanentKey

Request:
none

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "s_key_code":"47d8d60a474be711e2feb090bd266f614f50086433c383c7bb60ee29deb8c9992dec4606a6ae4f2535a69fd9b726a896bebbe15719438c76d74c8d539508d45ca7e2cef9702247192d4291f533786c819058f17d237696b934261b94e5598452fa4722b180ed0857031fdffec589485889e0328b2dce1a685430e7e9b3467e5e0c37da298bbe3261aa9eeb5551f7ae18bb95301d092fe2029bfa8c223448a7db1d469bbcd873ee9e3070ce4d8f9568"
  }
}
```

2.2.4 Retrieve Guest Key

Partner Server uses this API to get guest keys of specified lock. Guest keys can be used to lock/unlock the lock device, but have a time limit, also not able for reset operation.

Request URL	https://server.ip/ilocks/api/apps/v1/locks/:lockname/guestKey	
Request Method	PUT	
Header	Value	Note
Authorization	bearer <access-token>	<access-token> is returned by

		authentication	
Content-type	application/json		
Parameters	Required	Note	
start_time	Y	Effective start time of guest key, milliseconds from 1970-01-01 00:00:00	
end_time	Y	Effective end time of guest key, milliseconds from 1970-01-01 00:00:00	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	information
-- s_key_code	String	Y	encrypted guest key

Example:

PUT https://121.40.42.36/locks/api/apps/v1/locks/MJ000006/guestKey

Request:

```
{
  "end_time":1499658493401,
  "start_time":1499654893401
}
```

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "s_key_code":"47d8d60a474be711e2feb090bd266f614f50086433c383c7bb60ee29deb8c9992dec4606a6ae4f2535a69fd9b726a896c65b5a70e31bce5d5ced8e8ea79e58cfa7e2cef9702247192d4291f533786c81c398943360290c501e8b84c4b9f07bd1e4ba840d6f81db00de8aef8735376cea889e0328b2dce1a685430e7e9b3467e5e0c37da298bbe3261aa9eeb5551f7ae1e49170de9ef702a16d3d5bc21a690654d97e2699d987c48a598be738694fd1fcada5af4558f5153247b146603de215ea69432f5ac8b52f24c5bb2d4cc505d8aeabd59862b3e3bba3a603022487ed34a5"
  }
}
```


2.3 Gateway Operations

2.3.1 Retrieve All Gateways

Partner Server uses this API to get all gateways' basic information, which is required for later operations, i.e. retrieving gateway status.

Request URL	https://server.ip/ilocks/api/apps/v1/gateways		
Request Method	GET		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	
none	N		
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	JSON Array	Y	information
-- s_gateway_name	string	Y	Gateway name

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/gateways

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":[
    {"s_gateway_name":"XXXXXX"},
    {"s_gateway_name":"XXXXXX"}
  ]
}
```

2.3.2 Retrieve Gateway Status

Partner Server uses this API to get status of specified gateway, which is useful for checking whether gateway works normally.

Request URL	https://server.ip/ilocks/api/apps/v1/gateways/:gatewayName/status		
Request Method	GET		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	
none	N	Gateway has been specified in URL	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	information
-- l_last_heart_beat_time	long	Y	Gateway last heart beat time, milliseconds from 1970.

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/gateways/GW000001/status

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "l_last_heart_beat_time":1499656562651
  }
}
```

2.4 Lock Remote Operations

2.4.1 Retrieve Lock Status

Partner Server uses this API to get status of specified lock, which is useful for checking whether the lock works normally.

Request URL	https://server.ip/ilocks/api/apps/v1/locks/:lockName/status
Request Method	GET

Header	Value		Note
Authorization	bearer <access-token>		<access-token> is returned by authentication
Content-type	application/json		
Parameters	Required	Note	
none	N	Lock has been specified in URL.	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	information
-- i_signal	int	Y	Signal level of the lock
-- s_gateway_name	string	Y	Name of connected gateway
-- l_last_update_time	long	Y	Last update time, milliseconds from 1970

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/locks/UL000001/status

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "i_signal":-70
    "s_gateway_name":"GW000001",
    "l_last_update_time":1499656562651
  }
}
```

2.4.2 Setup Guest Password

Partner Server uses this API to send instruction to lock device, which will tell the device to setup a guest password. Users can unlock the device using the guest password.

Request URL	https://server.ip/ilocks/api/apps/v1/locks/:lockname/guestPasswdKey
Request Method	POST

Header	Value		Note
Authorization	bearer <access-token>		<access-token> is returned by authentication
Content-type	application/json		
Parameters	Required	Note	
start_time	Y	Effective start time of guest password, milliseconds from 1970-01-01 00:00:00	
end_time	Y	Effective end time of guest password, milliseconds from 1970-01-01 00:00:00	
local_start_time	N	Effective start time of guest password, local time: YYMMDDHHmm, i.e.1801021520	
local_end_time	N	Effective end time of guest password, local time: YYMMDDHHmm, i.e. 1801021520	
is_local_time	Y	0: use milliseconds; others: use local time, parameters local_start_time and local_end_time are required.	
one_time	Y	0: many times; others: only unlock 1 time.	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded; others: failed
msg	string	Y	Error messages
info	{}	Y	Collection
-- s_instruction_id	string	Y	Instruction ID
-- s_guest_passwd	string	Y	Guest Passowrd

NOTICE:

Actually, the guest password has not been setup yet when finishing the API call. Developers should check the instruction status (refer to 2.2.7) after the call according to the s_instruction_id returned by the call. If the status shows that the instruction has been executed successfully, then the guest password has been setup.

Example:

POST https://121.40.42.36/locks/api/apps/v1/locks/MJ000006/guestPasswdKey

Request:

none

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "s_instruction_id":"47d8d60a474be71"
    "s_guest_passwd":"123456"
  }}
}
```

2.4.3 Cancel Guest Password

Partner Server uses this API to send instruction to lock device, which will tell the device to cancel the existing guest password.

Request URL	https://server.ip/locks/api/apps/v1/locks/:lockname/guestPasswdKey		
Request Method	PUT		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	
guest_passwd	Y	Guest Passowrd	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	Collection
-- s_instruction_id	string	Y	Instruction ID

NOTICE:

Actually, the guest password has not been cancelled yet when finishing the API call. Developers should check the instruction status (refer to 2.2.7) after the call according to the s_instruction_id returned by the call. If the status shows that the instruction has been executed successfully, then the guest password has been cancelled.

Example:

PUT https://121.40.42.36/locks/api/apps/v1/locks/MJ000006/guestPasswdKey

Request:

none

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "s_instruction_id":"47d8d60a474be71"
  }
}
```

2.4.4 Remote Unlock

Partner Server uses this API to send instruction to lock device, which will tell the device to unlock immediately.

Request URL	https://server.ip/locks/api/apps/v1/locks/:lockname/remoteUnlock		
Request Method	PUT		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	
none	N	Parameter lockname has been specified in URL.	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	Collection
-- s_instruction_id	string	Y	Instruction ID

NOTICE:

Actually, the device has not been unlocked yet when finishing the API call. Developers should check the instruction status (refer to 2.2.7) after the call according to the s_instruction_id returned by the call. If the status shows that the instruction has been executed successfully, then the device has been unlocked.

Example:

PUT https://121.40.42.36/ilocks/api/apps/v1/locks/MJ000006/remoteUnlock

Request:

none

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "s_instruction_id":"47d8d60a474be71"
  }}
}
```

2.4.5 Retrieve Instruction Status

Partner Server uses this API to get the status of specified instruction.

Request URL	https://server.ip/ilocks/api/apps/v1/instruction		
Request Method	GET		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	
instruction_id	Y	Instruction ID returned by Operation response.	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages
info	{}	Y	Collection

-- i_status	int	Y	Instruction status.
-------------	-----	---	---------------------

Field i_status (instruction status) includes:

Value	Note
0x01	Succeeded to execute.
0x02	Failed to execute.
0x03	Instruction not pushed yet.
0x04	Failed to push instruction.
0x05	Instruction already pushed.

Example:

GET https://121.40.42.36/locks/api/apps/v1/instruction

Request:

```
{
  "instruction_id":"47d8d60a474be71"
}
```

Response:

```
{
  "ack":0,
  "msg":"succeed",
  "info":{
    "i_status":1
  }
}
```

2.5 Other Operations

2.5.1 Create Lock Keeper Account

Partner Server uses this API to create subaccount of APP Lock Keeper.

Request URL	https://server.ip/locks/api/apps/v1/users
Request Method	POST

Header	Value		Note	
Authorization	bearer <access-token>		<access-token> is returned by authentication	
Content-type	application/json			
Parameters	Required	Note		
	user_name	Y	Account name, start with characters.	
	user_password	Y	Account password, at least 6 characters.	
Returned Fields	Type	Required	Note	
ack	int	Y	0: succeeded, Others: failed	
msg	string	Y	Error messages	

Example:

GET https://121.40.42.36/ilocks/api/apps/v1/users

Request:

```
{
  "user_name": "testXXXX",
  "user_password": "XXXXXXXX"
}
```

Response:

```
{
  "ack": 0,
  "msg": "succeed",
}
```

2.5.2 Guest Key Sharing Callback

When other system, i.e. Hotel Server, needs to share a guest key through Lock Server, Partner Server may need to know about it and approve it (refer to session 1.6). In this case, Partner Server should setup this restful service, and provide the address to Lock Server when login (refer to session 2.1.1), then when sharing a guest key, Lock server will notify Partner Server by this callback immediately to approve it.

Notice again: this API is setup by Partner Server and called by Lock Server.

Request URL	Callback address provided when login		
Request Method	PUT		
Header	Value	Note	
Authorization	bearer <access-token>	<access-token> is returned by authentication	
Content-type	application/json		
Parameters	Required	Note	
key_code	Y	encrypted guest key	
start_time	Y	Effective start time of guest key, milliseconds from 1970-01-01 00:00:00	
end_time	Y	Effective end time of guest key, milliseconds from 1970-01-01 00:00:00	
Returned Fields	Type	Required	Note
ack	int	Y	0: succeeded, Others: failed
msg	string	Y	Error messages

Example:

PUT https://121.40.42.36/ilocks/api/apps/v1/locks/MJ000006/guestKey

Request:

```
{
  "key_code": "47d8d60a474be711e2feb090bd266f614f50086433c383c7bb60ee29deb8c9992dec4606a6ae4f2535a69fd9b726a896c65b5a70e31bce5d5ced8e8ea79e58cfa7e2cef9702247192d4291f533786c81c398943360290c501e8b84c4b9f07bd1e4ba840d6f81db00de8aef8735376cea889e0328b2dce1a685430e7e9b3467e5e0c37da298bbe3261aa9eeb5551f7ae1e49170de9ef702a16d3d5bc21a690654d97e2699d987c48a598be738694fd1fcada5af4558f5153247b146603de215ea69432f5ac8b52f24c5bb2d4cc505d8aeabd59862b3e3bba3a603022487ed34a5",
  "end_time": 1499658493401,
  "start_time": 1499654893401
}
```

Response:

```
{
  "ack": 0,
  "msg": "succeed",
}
```

}