



10Tacle Open API Design Specification

01 External Open API Interfacing Solution for 3rd access partners, such as facility booking system

Objective

To provide external interfaces for the maintenance of authorization information required by external systems to connect to the platform:

1. Add user extension portal
2. Add vehicle extension portal
3. Add external system access capability
4. Strengthen the security measures for external system access

Program Plan Phase I

Key management

New key management service, mainly for unified management of external access customer authentication mechanism Manage, assign and view interface authentication key information through the management background

Open api interfaces

User authorization

Create user authorization tasks by passing authentication elements, user elements, and device elements

Authentication elements

<AccessKey ID> + <AccessKey Secret>

User elements

<Country Code> + <Mobile Number> + [Profile]

Device element <Device Key>

Cancel user authorization task

Authentication elements

<AccessKey ID> + <AccessKey Secret>

User elements

<Country Code> + <Mobile Number>

Device Elements

<Device Key> Vehicle authorization

Create a vehicle authorization task by passing the authentication element, user element, device element, vehicle element

Authentication elements

<AccessKey ID> + <AccessKey Secret>

User elements

<Country Code> + <Mobile Number> + [Profile]

Device element <Device Key>

Vehicle element

<Vehicle Number>

Cancel vehicle authorization task

Authentication elements

<AccessKey ID> + <AccessKey Secret>

User elements

<Country Code> + <Mobile Number>

Device Elements

<Device Key>

Vehicle element

<Vehicle Number>

Section A

OPEN API GENERAL REQUEST INFO

Name Field	Data Type	Required	Remark
Version	String	Y	API version number, format: YYYY-MM-DD. Value: 2021-03-24
Timestamp	String	Y	Request Timestamp Based on ISO8601 standard, please use UTC timestamp, format: yyyy-MM-ddTHH:mm:ssZ. eg: 2018-01-01T12:00:00Z represent Singapore Time Year 2018 Month 01 Day 01 Hour 20 Min 00 Sec 00.
SignatureMethod	String	Y	Signature Method. Value: HMAC-SHA1.
SignatureNonce	String	Y	Unique Random Number For Signature. To protect unwanted network attack, we highly recommended use a different signature nonce for each api call, eg.89ebb339-63a6-4e29-85a7-2e501e721730
SignatureVersion	String	Y	Signature Algorithm Version.Value:1.0.
AccessKeyId	String	Y	Access Key ID. AccessKey to call API.

Action	String	Y	API Name
Signature	String	Y	Requested Signature Value. Refer to section B

API GENERAL RESPONSE INFO

Name Field	Type	Remark
RequestId	String	Request ID, no matter the api call success or fail there will be an id returned.
Success	Boolean	Whether api call is success. true means success, false means fail.
ErrorMessage	String	Error message when api call is failed
Code	String	Error code when api call is failed
Data	Object	Interface response data

Section B Request for signature

1. Specify request parameters

Specify the request parameters in the code. The parameters need to include the public request header and the necessary parameter information for the interface.

Parameters with Signature as the key are not allowed in the request parameters.

Sample Code:

```
params := make(map[string]string)

// common

params["Version"] = "2021-03-24"

params["Timestamp"] = "2021-03-24T14:31:56Z"

params["SignatureNonce"] = "89ebb339-63a6-4e29-85a7-2e501e721730"

params["SignatureVersion"] = "1.0"

params["SignatureMethod"] = "HMAC-SHA1"

params["AccessKeyId"] = "KJeCjxlwLYJwpiGHrZFgWVZn"

params["Action"] = "BindUserAndDevice"


// custom, which change with action

params["CountryCode"] = "65"

params["MobileNumber"] = "999999999"

params["DeviceKey"] = "LuCGqBV9W7UN"


// signature result : 5a067d76e5e10efecb00a6862ec626769dfb083c

signature := generateSignature(params)
```

2. Parameter handling

generateSignature Function, will include the following steps

- Convert QueryString one by one
- Special character handling
- Sort string array

```
// Convert every param into key=val format
```

```
queryStringArray := make([]string, len(params))
```

```
n := 0
```

```
for k, v := range params {
```

```
    queryStringArray[n] = k + "=" + SpecialUrlEncode(v)
```

```
    n++
```

```
}
```

```
// Sort the string array once to standardize and ensure that the encryption and
```

```
decryption sorts are consistent
```

```
sort.Strings(queryStringArray)
```

Please Note SpecialUrlEncode will add 3 more special char handling than

URLEncode

Replace + with %20

Replace * with %2A

Replace %7E with ~

3. Construct the request string to be signed

```
// Join the handled Query String Array from step 2 into a String
```

```
str := strings.Join(queryStringArray, "&")
```

4. Generate signature

AccessKeySecret will be assigned by platform, Please contact us for details

In this sample , eg. AccessKeySecret =

“awzZ12XHJjvyfAYpm8RjPO7U8Mt2eFWQ”

Sign through AccessKeySecret and plaintext to obtain signature

```
mac := hmac.New(sha1.New, []byte(AccessKeySecret))
```

```
mac.Write([]byte(str))
```

```
signature := hex.EncodeToString(mac.Sum(nil))
```

5. Add the signature result to the request parameters

```
// Add the final signature to the parameters
```


params["Signature"] = signature

6. Open Api -- Door/Vehicle Authorization/User Registration

To grant/remove mobile/Vehicle access for user from 3rd party system and allow using swipe for gate/barrier opening with 10Tacle APP/Swift with

License Plate Recognition

API Name :

BindUserAndDevice/UnbindUserAndDevice

BindVehicleAndDevice/UnBindVehicleAndDevice

RegistUser

Register Mobile User To 10Tacle Platform

Api Endpoint : /eco/api/iot

Api request:

Name Field	Data Type	Required	Remark
Version	String	Y	API version number, format: YYYY-MM-DD. Value: 2021-03-24

Timestamp	String	Y	Request Timestamp Based on ISO8601 standard, please use UTC timestamp, format: yyyy-MM-ddTHH:mm:ssZ. eg: 2018-01-01T12:00:00Z represent Singapore Time Year 2018 Month 01 Day 01 Hour 20 Min 00 Sec 00.
SignatureMethod	String	Y	Signature Method. Value: HMAC-SHA1.
SignatureNonce	String	Y	Unique Random Number For Signature. To protect unwanted network attack, we highly recommended use a different signature nonce for each api call, eg.89ebb339- 63a6-4e29-85a7-2e501e721730
SignatureVersion	String	Y	Signature Algorithm Version.Value:1.0.
AccessKeyId	String	Y	Access Key ID. AccessKey to call API.
Action	String	Y	RegistUser
Signature	String	Y	Requested Signature Value. Refer to section B
CountryCode	String	Y	International Mobile Country Code, eg. 65 for Singapore
MobileNumber	String	Y	User Mobile Number Eg. 999999999

Api Response

Name Field	Type	Remark
RequestId	String	Request ID, no matter the api call success or fail there will be an id returned.

Success	Boolean	Whether api call is success. true means success, false means fail.
ErrorMessage	String	Error message when api call is failed
Code	String	Error code when api call is failed
Data	Object	Interface response data

Add Mobile User Access

Api Endpoint : **/eco/api/iot**

Api request:

Name Field	Data Type	Required	Remark
Version	String	Y	API version number, format: YYYY-MM-DD. Value: 2021-03-24
Timestamp	String	Y	Request Timestamp Based on ISO8601 standard, please use UTC timestamp, format: yyyy-MM-ddTHH:mm:ssZ. eg: 2018-01-01T12:00:00Z represent Singapore Time Year 2018 Month 01 Day 01 Hour 20 Min 00 Sec 00.
SignatureMethod	String	Y	Signature Method. Value: HMAC-SHA1.
SignatureNonce	String	Y	Unique Random Number For Signature. To protect unwanted network attack, we highly recommended use a different signature nonce

			for each api call, eg.89ebb339-63a6-4e29-85a7-2e501e721730
SignatureVersion	String	Y	Signature Algorithm Version.Value:1.0.
AccessKeyId	String	Y	Access Key ID. AccessKey to call API.
Action	String	Y	BindUserAndDevice
Signature	String	Y	Requested Signature Value. Refer to section B
CountryCode	String	Y	International Mobile Country Code, eg. 65 for Singapore
MobileNumber	String	Y	User Mobile Number Eg. 999999999
DeviceKey	String	Y	10Tacle IoT Device Key Eg. LuCGqBV9W7UN

Api Response

Name Field	Type	Remark
RequestId	String	Request ID, no matter the api call success or fail there will be an id returned.
Success	Boolean	Whether api call is success. true means success, false means fail.
ErrorMessage	String	Error message when api call is failed
Code	String	Error code when api call is failed
Data	Object	Interface response data

Remove Mobile User Access

Api Endpoint : /eco/api/iot

Api request:

Name Field	Data Type	Required	Remark
Version	String	Y	API version number, format: YYYY-MM-DD. Value: 2021-03-24
Timestamp	String	Y	Request Timestamp Based on ISO8601 standard, please use UTC timestamp, format: yyyy-MM-ddTHH:mm:ssZ. eg: 2018-01-01T12:00:00Z represent Singapore Time Year 2018 Month 01 Day 01 Hour 20 Min 00 Sec 00.
SignatureMethod	String	Y	Signature Method. Value: HMAC-SHA1.
SignatureNonce	String	Y	Unique Random Number For Signature. To protect unwanted network attack, we highly recommended use a different signature nonce for each api call, eg.89ebb339-63a6-4e29-85a7-2e501e721730
SignatureVersion	String	Y	Signature Algorithm Version.Value:1.0.
AccessKeyId	String	Y	Access Key ID. AccessKey to call API.
Action	String	Y	UnBindUserAndDevice
Signature	String	Y	Requested Signature Value. Refer to section B
CountryCode	String	Y	International Mobile Country Code, eg. 65 for Singapore

MobileNumber	String	Y	User Mobile Number Eg. 999999999
DeviceKey	String	Y	10Tacle IoT Device Key Eg. LuCGqBV9W7UN

Api Response

Name Field	Type	Remark
RequestId	String	Request ID, no matter the api call success or fail there will be an id returned.
Success	Boolean	Whether api call is success. true means success, false means fail.
ErrorMessage	String	Error message when api call is failed
Code	String	Error code when api call is failed
Data	Object	Interface response data

Add Vehicle User Access

Api Endpoint : /eco/api/iot

Api request:

Name Field	Data Type	Required	Remark
Version	String	Y	API version number, format: YYYY-MM-DD. Value: 2021-03-24
Timestamp	String	Y	Request Timestamp Based on ISO8601 standard, please use UTC timestamp, format: yyyy-MM-ddTHH:mm:ssZ. eg: 2018-01-01T12:00:00Z represent Singapore Time Year 2018 Month 01 Day 01 Hour 20 Min 00 Sec 00.
SignatureMethod	String	Y	Signature Method. Value: HMAC-SHA1.
SignatureNonce	String	Y	Unique Random Number For Signature. To protect unwanted network attack, we highly recommended use a different signature nonce for each api call, eg.89ebb339-63a6-4e29-85a7-2e501e721730
SignatureVersion	String	Y	Signature Algorithm Version.Value:1.0.
AccessKeyId	String	Y	Access Key ID. AccessKey to call API.
Action	String	Y	BindVehicleAndDevice
Signature	String	Y	Requested Signature Value. Refer to section B
VehicleNumber	String	Y	User Vehicle Number Eg. SLS121S

DeviceKey	String	Y	10Tacle IoT Device Key Eg. LuCGqBV9W7UN
-----------	--------	---	--

Api Response

Name Field	Type	Remark
RequestId	String	Request ID, no matter the api call success or fail there will be an id returned.
Success	Boolean	Whether api call is success. true means success, false means fail.
ErrorMessage	String	Error message when api call is failed
Code	String	Error code when api call is failed
Data	Object	Interface response data

Remove Vehicle User Access

Api Endpoint : /eco/api/iot

Api request:

Name Field	Data Type	Required	Remark
Version	String	Y	API version number, format: YYYY-MM-DD. Value: 2021-03-24
Timestamp	String	Y	Request Timestamp Based on ISO8601 standard, please use UTC timestamp, format: yyyy-MM-ddTHH:mm:ssZ. eg: 2018-01-01T12:00:00Z represent Singapore Time Year 2018 Month 01 Day 01 Hour 20 Min 00 Sec 00.
SignatureMethod	String	Y	Signature Method. Value: HMAC-SHA1.
SignatureNonce	String	Y	Unique Random Number For Signature. To protect unwanted network attack, we highly recommended use a different signature nonce for each api call, eg.89ebb339-63a6-4e29-85a7-2e501e721730
SignatureVersion	String	Y	Signature Algorithm Version.Value:1.0.
AccessKeyId	String	Y	Access Key ID. AccessKey to call API.
Action	String	Y	UnBindVehicleAndDevice
Signature	String	Y	Requested Signature Value. Refer to section B
VehicleNumber	String	Y	User Vehicle Number Eg. SLS121S

DeviceKey	String	Y	10Tacle IoT Device Key Eg. LuCGqBV9W7UN
-----------	--------	---	--

Api Response

Name Field	Type	Remark
RequestId	String	Request ID, no matter the api call success or fail there will be an id returned.
Success	Boolean	Whether api call is success. true means success, false means fail.
ErrorMessage	String	Error message when api call is failed
Code	String	Error code when api call is failed
Data	Object	Interface response data