

NISSAN MOTOR CORPORATION



MAC Key Unlocking Solution- user guide

Version 1.0

2022/04/14

revision history

#	Date	Version	Modification details.		
1	2022/02/13	0.90 Draft	create a new		
2	2022/04/04	0.91 Draft	SLA updated (Performance)	OLD	NEW
				Within 5 secs.	getProductionPlantMacKey Within 15 secs. Other: Within 5 secs.
3	2022/04/14	1.0	Sample request and responses updated Pg 5~12		

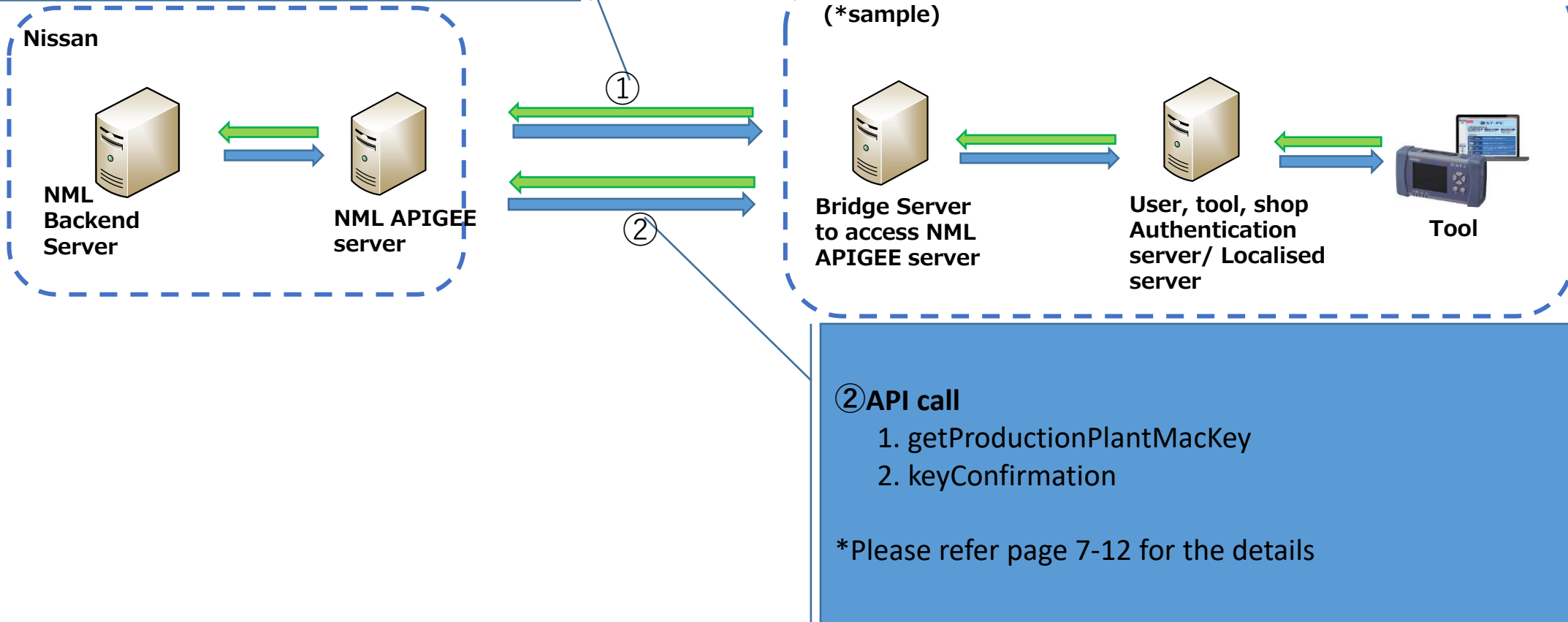
① NML APIGEE Access (Server to Server access):

Below information will be required to access the NML APIGEE server access (will be provided by NML)

1. Access URL,
2. key,
3. secret,

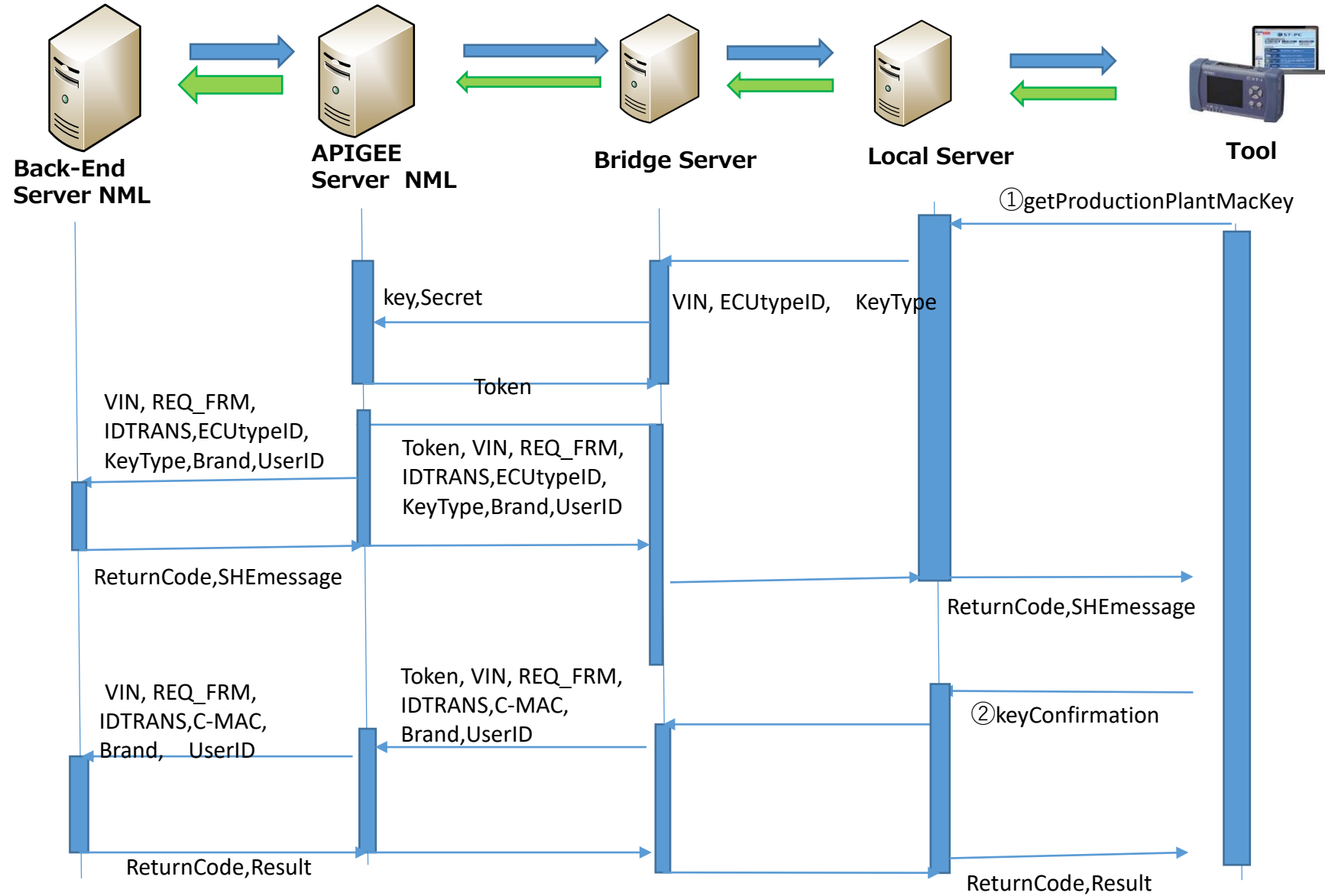
*Please refer page 5-6 for details.

System architecture



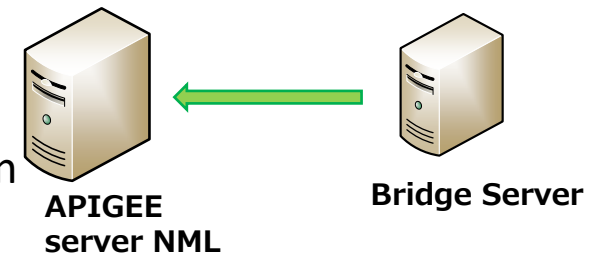
* Regarding system security requirements please refer page 13

Data Flow Sequence diag.



Token Access Request

=> API Clients call APIGEE in order to authenticate by OAuth2.0. =>
Acquire Access token by accessing by setting necessary parameters in
the following URL



Request URL

<https://api-qa.nissan-europe.com/identity/v2/token>

	Parameter	Mandatory/O ptional	値
HTTP Header	HTTP Method	Mandatory	"GET"
	Content-Type	Mandatory	"application/x-www-form-urlencoded"
	Authorization	Mandatory	Basic <Base64(Key:Secret*)>
HTTP Body	grant_type	Mandatory	"client_credentials"

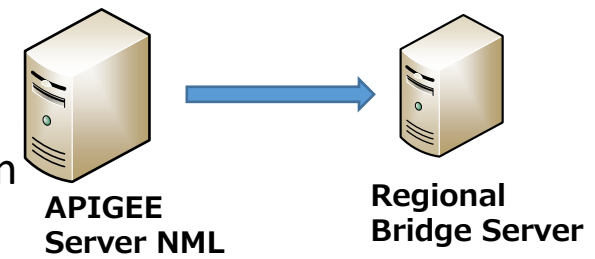
Example :

GET <https://api-qa.nissan-europe.com/identity/v2/token>

* key, secret will be created and sent by NML team.

Access Token Response

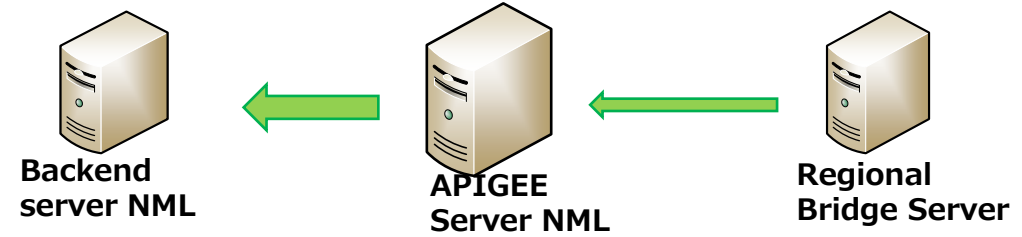
=> API Clients call APIGEE in order to authenticate by OAuth2.0. =>
Acquire Access token by accessing by setting necessary parameters in
the following URL



	Parameter	sucess	Error	value
HTTP Header	Status code	mandatory	mandatory	Status code by process result in APIGEE
	Content-Type	mandatory	mandatory	"application/json;charset=UTF-8"
	Cache-Control	mandatory	mandatory	"no-cache,no-store,no-transform,must-revalidate"
	Pragma	mandatory	mandatory	"no-cache"
	X-unique-id	optional	optional	Value by request from API Client
HTTP Body	access_token	mandatory	No use	If authentication is success, access token is set by API GEE
	token_type	mandatory	No use	"Bearer"
例				
Success	{ "token": "7UKJOWxWRddjXv5LGgbMABDpR0CM" }			
Error	{ "code": "401.01.01", "message": "Invalid credentials", "info": "Invalid client credentials" }			

① API Request

=> API Client invokes the API provider's API using the access token.



Request URL			
<a href="https://api-qa.nissan-europe.com/dealers/v1/diagInfo/vin/[VINXXXXXXXXXXXXXX]/productionPlantMacKey?<Query Parameter>">https://api-qa.nissan-europe.com/dealers/v1/diagInfo/vin/[VINXXXXXXXXXXXXXX]/productionPlantMacKey? <Query Parameter>			
	Parameter	Manadatory/O ptional	Value
HTTP Header	HTTP Method	Mandatory	Get
	Authorization Type	Mandatory	Oauth2.0
	Authorization	Mandatory	"Bearer " token
	Content-Type	Optional	Application/json
Query Parameter	Depends on specification of API Provider	Mandatory	REQ_FRM=[REQFRM]& IDTRANS=[IDTRANS]& ECUtypeID=[ECUtypeid]& KeyType=[keytype]& Brand=ADTN& UserID=[userid]
HTTP Body	Depends on specification of API Provider	Optional	None
https://api-qa.nissan-europe.com/dealers/v1/diagInfo/vin/VINXXXXXXXXXXXXXX/productionPlantMacKey?REQ_FRM=CS3P&IDTRANS=LOADDIAGTEST202203211942&ECUtypeID=xxxxxxx&KeyType=0&Brand=ADTN&UserID=FJT01008			

① getProductionPlantMacKey Request

	Tag name	Description	Max Length	Mandatory	Conversion/Comment
1	VIN	Vehicle Identity Number (17 char ASCII)	17	Mandatory	- When VIN is less than 17 characters, then left padding with 0 (zero) and hyphen conversion to 0 must be done at client side and sent. e.g. Original VIN VNK-123456 will be converted to 0000000VNK0123456 and sent to SDR
2	REQ_FRM	Company name (*TBD)	10	Mandatory	
3	TRANSACTION ID	max 24 char. Unique for each request	24	Mandatory	Unique id for traceability purpose TBD
4	ECUtypeID	GP(Generic Part Number)	9	Mandatory	
5	KeyType	0 : for K_master_ECU 1 : for K_mac	1	Mandatory	
6	Brand	ADTN	4	Mandatory	
7	Tool_ID	PC serial id	128	Mandatory	
8	Location/region	Country code	5	Mandatory	
9	Tool login User id	user identification num	20	Mandatory	

*TBD: will be decided mutually after application to NML

Sample Request :

[https://api-ga.nissan-europe.com/dealers/v1/diagInfo/vin/VINXXXXXXXXXXXXXX/productionPlantMacKey?](https://api-ga.nissan-europe.com/dealers/v1/diagInfo/vin/VINXXXXXXXXXXXXXX/productionPlantMacKey?REQ_FRM=CS3P&IDTRANS=LOADDIAGTEST202203211942&ECUtypeID=xxxxxxx&KeyType=0&Brand=ADTN&UserID=FJT01008)

REQ_FRM=CS3P&

IDTRANS=LOADDIAGTEST202203211942&

ECUtypeID=xxxxxxx&

KeyType=0&

Brand=ADTN&

UserID=FJT01008

②keyConfirmation Request

	Tag name	Description	Max Length	Mandatory	Conversion/Comment
1	VIN	Vehicle Identity Number (17 char ASCII)	17	Mandatory	- When VIN is less than 17 characters, then left padding with 0 (zero) and hyphen conversion to 0 must be done at client side and sent. e.g. Original VIN VNK-123456 will be converted to 0000000VNK0123456 and sent to SDR
2	REQ_FRM	Company name (*TBD)	10	Mandatory	
3	TRANSACTION ID	max 24 char. Unique for each request	24	Mandatory	Unique id for traceability purpose TBD
4	C-MAC	C-MAC(16byte): Encrypted by ECU K MAC *1 <i>Note1: *1 is binary data. the data should be encoded by BASE64 and be set as an input data.</i>	24	Mandatory	
5	Brand	ADTN	4	Mandatory	Fixed value
6	Tool_ID	PC serial id	128	Mandatory	
7	Location/region	Country code	10	Mandatory	
8	Tool login User id	user identification number	20	Mandatory	

*TBD: will be decided mutually after application to NML

Sample Request :

<https://api-ga.nissan-europe.com/dealers/v1/diagInfo/vin/VINXXXXXXXXXXXXX/keyConfirmation?>

REQ_FRM=CS3P&

IDTRANS=LOADDIAGTEST202203211942&

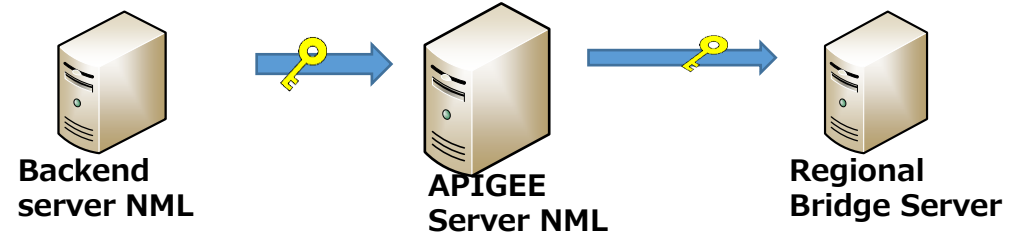
Brand=ADTN&

UserID=FJT01008&

C-MAC=p2WeWFZBC6vr3oG6WDabWQ==

① API Response

=> API Gateway passes the response received from API Provider to API Client as it is..



	Parameter	Success	Error	value
HTTP Header	Status code/Response Phase	mandatory	mandatory	Depends on the processing result.
	Content-Type	mandatory	mandatory	Application/json
	Cache-Control	mandatory	mandatory	"no-cache,no-store,no-transform,must-revalidate"
	Pragma	mandatory	mandatory	"no-cache"
	Content-Length	mandatory	mandatory	Depends on the processing result.
	X-unique-id	optional	optional	Value by request from API Client.
HTTP Body	Depends in API Provider	mandatory	mandatory	Detail is Explained in the next page
Sample				
success				
Error				

①getProductionPlantMacKey Response

	Tag name	Description	Max Length	Mandatory	Conversion/Comment
1	ReturnCode	Code for success or error as returned from backend.	8	Mandatory	
2	SHEmessage	SHE message (M1, M2, M3): M1(16 byte)+M2(32byte)+M3(16byte) *1 <i>Note1: *1 is binary data. the data should be encoded by BASE64 and be set as an output data.</i> <i>Note2: If "ReturnCode" is NG value, this parameter is NOT set in an error response.</i>	88	Mandatory	

*TBD: will be decided mutually after application to NML

Sample Response :

```
{
  REQUESTRESPONSE:{"REQUEST":{"HEADER":{"REQ_TO":"SDR","REQ_SYSTEM_SPECIFIC":{"PC_SERIAL_ID":"FJT02126","REQUEST_TYPE":"ADT3REST"},"ERRORS":{"ERROR":[]},"REQ_FRM":"CS3P"},"CONTENTS":{"VIN":["VIN"],"ecu":{},"IDTRANS":["IDTRANS"],"API_TYPE":"getProductionPlantMacKey","REQ_JSON":{"
    "VIN": "[VIN]",
    "ECUtypeID": "xxxxxxx",
    "KeyType": "0",
    "Brand": "ADTN",
    "UserID": "FJT02126"
  }}},"RESPONSE":{"HEADER":{"ERRORS":{"ERROR":{"RCODE":"00","REASCODE":"00000"}}},"CONTENTS":{"R
ESP_JSON":{"
    "ReturnCode": "MAC_C000",
    "SHEmessage": "AAAAAAAAAAAA.....XXXX"
  }}}}}
```

②keyConfirmation Response

	Tag name	Description	Max Length	Mandatory	Conversion/Comment
1	ReturnCode	Code for success or error as returned from backend.	8	Mandatory	
2	Result	0 default 1 current key 2 new key 3 unknown Note: If "ReturnCode" is NG value, this parameter is NOT set in an error response.	1	Mandatory	

*TBD: will be decided mutually after application to NML

Sample Response :

```
{
  REQUESTRESPONSE:{"REQUEST":{"HEADER":{"REQ_TO":"SDR","REQ_SYSTEM_SPECIFIC":{"PC_SERIAL_ID":"C3P12345678901234567890a","REQUEST_TYPE":"ADT3REST"},"ERRORS":{"ERROR":[]},"REQ_FRM":"CS3P"},"CONTENTS":{"VIN":"GPC00000AL4498061","ecu":{},"IDTRANS":"FJT02126_100351341548","API_TYPE":"keyConfirmation","REQ_JSON":{"VIN": "GPC00000AL4498061",
"C-MAC": "p2WeWFZBC6vr3oG6WDabWQ==",
"KeyType": "0",
"Brand": "ADTN",
"UserID": "FJT01008"
}}},"RESPONSE":{"HEADER":{"ERRORS":{"ERROR":[{"RCODE":"00","REASCODE":"00000"}]}}, "CONTENTS":{"RESP_JSON":{"Result": 0,
"ReturnCode": "MAC_C000"
}}}}}}
```

Security requirements :

1. Server to Server access :

API access must be from a centralized server(Bridge server) not directly from the diagnostic tools

2. Tool id & Tool User Id authentication :

The central server must identify the tool and the users accessing the tool for traceability purpose.
Authentication and authorization must be done on vendor side.

The user id and tool id must be sent in the request (Tool id , Tool login User id)

* Please refer page 7 & 8

3. Access log :

The central server must keep the access log of Tool id and Tool user id for request and response for traceability purpose.

4. Access to NML APIGEE server :

NML APIGEE server uses OAuth 2.0 for accessing to backend API.

In First step Client id, client secret and certificate is sent to NML APIGEE server to get token.

In second step, Token is used along with API parameters to access the backend API.

*Certificate will expire in 1 year. New certificate will be issued one month before expiry of the certificate

5. Below documents to be submitted:

1. SISA document to be filled in by supplier [No Japanese version available]
2. ISO 27001 certification or SASE Service Organization Control (SOC) report if available
3. Detailed service description provided by vendor to Nissan

Information to be shared from NML :

1. Access URL (Test and prod):

NML APIGEE server and Backend servers have both test and production environments. Production access will be provided after successful tests in test environment.

2. Certificate (Test and prod):

Certificates for NML APIGEE server access will be provided for both test and production environments.

3. Client ID, Client Secret(Test and prod)

Client Id, Client secret for NML APIGEE server access will be provided for both test and production environments.

4. Request parameter

Company code & Region code will be decided and informed after discussions.

5. Sample

Sample JSON request and response for the API will be provided.

6. Return code list

Return code list (success and error codes returned from backend) will be provided.

Topic	Description	Service Level/Duration	Scope
Service Availability (Production)	Backend Service Availability	99.5% Uptime(Considering Planned maintenance and Planned maintenance with notice)	This service level only backend system service and includes below components : Hardware, operating system, backend application, backend DB.
Performance	Backend Service Response Time	getProductionPlantMacKey Within 15 secs. Other: Within 5 secs.	Response time is for backend response time only. It doesn't contain response include response time of API Gateway and network outside of Nissan.
Planned Maintenance	Production	4th Monday of Month 01:00 to 03:00 JST	
	QA	3rd Monday of Month 01:00 to 03:00 JST	
Planned Maintenance with Notice	Update firmware for hardware and middleware version	Quarterly 4 times in a year Working hours : Approx. 5 hrs.	
Application Level	Application Importance Level	3	Backend Application
Technical Incident Management	Support Hours	9:00 to 18:00 JST *** 5 days a week (Nissan Holidays excluded)	Support by Email***
	Reaction Time	9:00 to 18:00 JST *** 5 days a week (Nissan Holidays excluded)	Support by Email***

Tentative Schedule:

FYXX												
	Week 1	Week 2	Week 3	---	---	---	---	---	---	---	---	---
Agreement completion												
NML IS	Agree with I/F spec with Q&A											
	Application to APIGEE infra team	Backend settings Update QA					Backend settings Update PROD					
NML INFRA		APIGEE Settings (QA)				APIGEE Settings (PROD)						
USER				Testing in QA				E2E Testing in PROD				

①getProductionPlantMacKey

request:

```
SDR/giagnosis/{vin}/mac-key?REQ_FRM="ReqFrm", "IDTRANS":  
"C3P12345678901234567890", "ECUtypeID": "R2370008-  
", "KeyType": 0, "Brand": "1", "UserID": "",
```

Response:

```
'{"ReturnCode":"MAC_C000", "SHEmessage":"34AE45BC...A5B5  
"}'
```

②keyConfirmation

Request:

```
SDR/giagnosis/{vin}/key-confirmation?REQ_FRM="ReqFrm",  
"IDTRANS": "C3P12345678901234567890", "C-  
MAC": "XXXXXX...XXX", "Brand": "1", "UserID": "",
```

Response:

```
'{"ReturnCode":"MAC_C000", "Result":0}'
```