NKM 솔루션 연동 Tier API 가이드

개정 이력

생성일	Version	개정 이력	비고
2025.10.17	1.0	• 최초 작성	

1. EcuID

Supplier 키 정보 등록(supplierKey) POST "/app/automotive/supplierEcuID"

REQUEST BODY			
field	**type**	**required**	**description**
EcuType	String	O	ECU Type
Phase	String	O	Phase(Dev, Prod)
SupplierID	String	O	SupplierID (스펙문서 참고)
EcuID	String	O	ECU ID (스펙문서 참고)
Serial	String	O	키 관리용 시리얼 넘버

RESPONSE BODY		
field	**type**	**description**
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)
Records	Json	결과 값 (M1~M5, KeySyncValue)

• REQ) Example

```
1  {
2      "SupplierID": "00",
3      "EcuType" : "00",
4      "Phase": "Dev",
5      "EcuID": "0102030405060708010203040003000100000000000000000000002",
6      "Serial": "Serial_1111111"
```

```
7  }
```

- RES) Example

```
1  {
2      "ResultStatus": "Success",
3      "ResultReason": "",
4      "ResultMessage": ""
5  }
```

2. MasterECUKey

키 프로비저닝(MasterECUKey) POST "/app/automotive/supplierKeyProvisioning"

REQUEST BODY			
field	type	required	description
ProvisioningType	String	O	Provisioning Type - Master ECU Key : EcuMasterKey - Supplier ECU symmetric Identity Key : SupplierSymmKey - SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
KeyID	String	O	Key ID (스펙문서 참고) (0x1)

RESPONSE BODY		
field	type	description
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)
Records	Json	결과 값 (M1~M5, KeySyncValue)

- REQ) Example

```
1  {
2    "ProvisioningType": "EcuMasterKey",
3    "KeyID": "1",
4    "EcuID": "0102030405060708010203040003000100000000000000000000002"
5  }
```

- RES) Example

```
1      "Records": {
2        "KeyID": "1",
3        "M1": "0003000100000000000000000000000211",
4        "M2": "83a6957a7c21c35c9bf9083c09c728fa8ebb3965805bfe8f9fd6b88b7fcf8df4",
5        "M3": "1eae814952a1ad6f9efc2e0c20378c3d",
6        "M4": "00030001000000000000000000000000002119d65cbf811941c12318183fce05f9880",
7        "M5": "adf3b9cb4e14a5cb60899f1a4a59feb2"
8      },
9      "ResultMessage": "",
10     "ResultReason": "",
11     "ResultStatus": "Success"
12   }
```

키 프로비저닝 주입 결과(MasterECUKey) PUT "/app/automotive/supplierKeyProvisioning"

REQUEST BODY			
field	**type**	**required**	**description**
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
ResultMessage	String	O	결과 메시지
ResultStatus	String	O	결과 상태 (Success, OperationFailed)

RESPONSE BODY		
field	**type**	**description**
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)

- REQ) Example

```
1  {
2    "ProvisioningType": "SupplierSymmKey",
3    "EcuID": "010203040506070801020304000001001D0102030405060708090A0B",
4    "ResultMessage": "",
5    "ResultStatus": "Success"
6  }
```

- RES) Example

```
1  {
2    "ResultStatus": "Success",
3    "ResultReason": "",
4    "ResultMessage": ""
5  }
```

3. SupplierSymmKey

키 프로비저닝(SupplierSymmKey) POST **"/app/automotive/supplierKeyProvisioning"**

REQUEST BODY			
field	**type**	**required**	**description**
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
KeyID	String	O	Key ID (스펙문서 참고) (0xD)

RESPONSE BODY		

field	type	description
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)
Records	Json	결과 값 (M1~M5, KeySyncValue)

- REQ) Example

```
1  {
2    "ProvisioningType": "SupplierSymmKey",
3    "KeyID": "D",
4    "EcuID": "01020304050607080102030400030001000000000000000000000002"
5  }
```

- RES) Example

```
1  {
2    "ResultStatus": "Success",
3    "ResultReason": "",
4    "ResultMessage": "",
5    "Records": {
6      "M1": "0001001d0102030405060708090a0b01",
7      "M2": "c723139a9975ad356707be66689de4cb4be6b9564b06bdc220c3b5328677d02b",
8      "M3": "0ccae90a3fc9b4ea06a578f58710d488",
9      "M4": "0001001d0102030405060708090a0b01b472e8d8727d70d57295e74849a27917",
10     "M5": "0ee0763aec1f41ce57bdd33bf9fe6e36"
11   },
12 }
```

키 프로비저닝 주입 결과(SupplierSymmKey) PUT "/app/automotive/supplierKeyProvisioning"

REQUEST BODY			
field	**type**	**required**	**description**
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
ResultMessage	String	O	결과 메시지
ResultStatus	String	O	결과 상태 (Success, OperationFailed)

RESPONSE BODY		
field	**type**	**description**
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)

- REQ) Example

```
1  {
2    "ProvisioningType": "SupplierSymmKey",
3    "EcuID": "0102030405060708010203040001001D0102030405060708090A0B",
4    "ResultMessage": "",
5    "ResultStatus": "Success"
```

```
6  }
```

- RES) Example

```
1  {
2    "ResultStatus": "Success",
3    "ResultReason": "",
4    "ResultMessage": ""
5  }
```

키 SyncValue 요청(SupplierSymmKey) POST "/app/automotive/supplierKeySyncValue"

REQUEST BODY			
field	type	required	description
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)

RESPONSE BODY		
field	type	description
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)
Records	Json	결과 값 (KeySyncValue, Challenge)

- REQ) Example

```
1  {
2    "ProvisioningType": "SupplierSymmKey",
3    "KeyID": "D",
4    "EcuID": "01020304050607080102030400030001000000000000000000000002"
5  }
```

- RES) Example

```
1   {
2     "Records": {
3       "KeyID": "",
4       "KeySyncValue": "e3a45734090e095e647ad21477120710",
5       "Challenge": "f6daf9cb30419105c64d27857da69f6b"
6     },
7     "ResultMessage": "",
8     "ResultReason": "",
9     "ResultStatus": "Success"
10  }
```

키 SyncValue 검증 결과(SupplierSymmKey)PUT "/app/automotive/supplierKeySyncValue"

REQUEST BODY			
field	type	required	description
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey

			• Supplier ECU symmetric Identity Key : SupplierSymmKey
			• SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
ResultMessage	String	O	결과 메시지
ResultStatus	String	O	결과 상태 (Success, OperationFailed)

RESPONSE BODY		
field	type	description
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)

- REQ) Example

```
1  {
2    "ProvisioningType": "SupplierSymmKey",
3    "EcuID": "01020304050607080102030400001001D0102030405060708090A0B",
4    "ResultMessage": "",
5    "ResultStatus": "Success"
6  }
```

- RES) Example

```
1  {
2    "ResultStatus": "Success",
3    "ResultReason": "",
4    "ResultMessage": ""
5  }
```

4. SecOCKey

키 프로비저닝(SecOCKey) POST "/app/automotive/supplierKeyProvisioning"

REQUEST BODY			
field	type	required	description
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
KeyID	String	O	Key ID (스펙문서 참고) (0x4~0xC)
SupplierSecretKey	String	O	협력사 SecretKey
Counter	String	O	Counter
Challenge	String	O	Constant Value 16byte

RESPONSE BODY		
field	type	description

ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)
Records	Json	결과 값 (M1~M5, KeySyncValue)

- REQ) Example

```
1  {
2    "ProvisioningType": "SecOCKey",
3    "EcuID": "010203040506070801020304000300010000000000000000000002",
4    "KeyID": "4"
5    }
```

- RES) Example

```
1   {
2     "Records": {
3       "KeyID": "5",
4       "M1": "0003000100000000000000000000000251",
5       "M2": "16d4ca7b74b48dafefdae7ade95eacbe5851dad0b3c5f6b319b2b12ccb4242a3",
6       "M3": "91ec2cf7188e7749cde1890067415d65",
7       "M4": "0003000100000000000000000000000251ffddafb77dcc9cf295a0fe25ade4f8ad",
8       "M5": "6715a001327a4149e8b6af665e188b22"
9     },
10    "ResultMessage": "",
11    "ResultReason": "",
12    "ResultStatus": "Success"
13  }
```

키 프로비저닝 주입 결과(SecOCKey) PUT "/app/automotive/supplierKeyProvisioning"

REQUEST BODY			
field	**type**	**required**	**description**
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
KeyID	String	O	SHE Key Slot ID (SecOC Cluster Key's ID = 0x4~0xC)
ResultMessage	String	O	결과 메시지
ResultStatus	String	O	결과 상태 (Success, OperationFailed)

RESPONSE BODY		
field	**type**	**description**
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)

- REQ) Example

```
1  {
2    "ProvisioningType": "SecOCKey",
3    "EcuID": "010203040506070801020304000100 1D0102030405060708090A0B",
4    "KeyID": "4",
```

```
5    "ResultMessage": "",
6    "ResultStatus": "Success"
7  }
```

- RES) Example

```
1  {
2    "ResultStatus": "Success",
3    "ResultReason": "",
4    "ResultMessage": ""
5  }
```

키 SyncValue 요청(SecOCKey) POST "/app/automotive/supplierKeySyncValue"

REQUEST BODY			
field	type	required	description
ProvisioningType	String	O	Provisioning Type • Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)

RESPONSE BODY		
field	type	description
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)
Records	Json	결과 값 (KeySyncValue, Challenge)

- REQ) Example

```
1  {
2    "ProvisioningType": "SecOCKey",
3    "EcuID": "01020304050607080102030400030001000000000000000000000002",
4    "KeyID": "4"
5  }
```

- RES) Example

```
1  {
2    "Records": {
3      "KeyID": "4",
4      "KeySyncValue": "db12bea12e44b066bca2dd8c7e1da577",
5      "Challenge": "FFFF5A5A5A5A5A5A5A5A5A5A5A5A5AFFFF"
6    },
7    "ResultMessage": "",
8    "ResultReason": "",
9    "ResultStatus": "Success"
10 }
```

키 SyncValue 검증 결과(SecOCKey)PUT "/app/automotive/supplierKeySyncValue"

REQUEST BODY			
field	type	required	description
ProvisioningType	String	O	Provisioning Type

			• Master ECU Key : EcuMasterKey • Supplier ECU symmetric Identity Key : SupplierSymmKey • SecOC Cluster Key : SecOCKey
EcuID	String	O	ECU ID (스펙문서 참고)
KeyID	String	O	SHE Key Slot ID (SecOC Cluster Key's ID = 0x4~0xC)
ResultMessage	String	O	결과 메시지
ResultStatus	String	O	결과 상태 (Success, OperationFailed)

RESPONSE BODY		
field	**type**	**description**
ResultStatus	String	결과상태(Success,OperationFailed)
ResultReason	String	결과코드(결과상태 Success → blank)
ResultMessage	String	결과메시지(결과상태 Success → blank)

- REQ) Example

```
1  {
2    "ProvisioningType": "SecOCKey",
3    "EcuID": "0102030405060708010203040001001D0102030405060708090A0B",
4    "KeyID": "4",
5    "ResultMessage": "",
6    "ResultStatus": "Success"
7  }
```

- RES) Example

```
1  {
2    "ResultStatus": "Success",
3    "ResultReason": "",
4    "ResultMessage": ""
5  }
```

5. 오류 메시지 및 대응 방법

메시지	설명	대응 방법	비고
The [　　] is required.	필수 입력 속성이나 타입 데이터가 없거나 빈 값	필수 입력 속성이나 타입을 입력 ex> The KeyID is required. 　　　KeyID = "";　→ KeyID = "4";	

The [　　] is not registerd.	해당 속성의 데이터가 KMS 에 등록되지 않음	해당 속성이나 타입이 KMS 에 등록되있는지 확인 후 없으면 등록
		ex> The SupplierID is not registerd.
		　　SupplierID="3D"　→　SupplierID="0D" // 실제 등록된 SupplierID 으로
		ex> EcuType="09" → EcuType="01"
		　(위 처럼 NKM에 설정된 제어기로 설정하거나 NKM 에 제어기 추가 등록)
		
		< 웹콘솔의 '협력사 & 제어기' 메뉴 화면 >
		
		협력사　　제어기　　협력사의 제어기에 대한 ID
		　　　　　VPC　　　0001
		　　　　　SBW_SHIFTER　0002	

keyID Parsing Err : [　　]	keyID 형식이 잘못됨	KeyID을 형식에 맞게 수정 ex> KeyID = "ㅎㄷ"; → KeyID = "C";	
The KeyID must be less than or equal to D(0x0D).	keyID 범위 (0~D) 를 벗어난 입력 값	KeyID을 범위에 맞게 수정 ex> KeyID = "3C"; → KeyID = "C";	
Phase = ([Prod] or [Dev]): [　]	Phase 값이 Prod, Dev 둘 중 하나로 입력되지 않음	Phase 값을 Prod, Dev 둘 중 하나로 입력 Phase = "Test"; → Phase = "Prod";	
The SupplierSecretKey:[　　] is not registerd.	OEM 으로부터 SupplierSecretKey 를 공유받지 않음	OEM 으로부터 SupplierSecretKey 를 공유 요청 및 키를 공유음	