密钥管理系统

TCCLI 管理指南

产品文档

腾讯云

文档目录

TCCLI 管理指南
操作总览

最近更新时间：2024-01-11 16:28:54

您可以调用 KMS TCCLI 管理密钥，例如创建密钥、查看密钥 ID 列表、编辑密钥、密钥轮换等操作。
操作使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

操作	说明
创建密钥	提供示例介绍如何调用 TCCLI 创建密钥
查看密钥	提供示例介绍如何调用 TCCLI 查看密钥 ID 和详情信息
编辑密钥	提供示例介绍如何调用 TCCLI 编辑密钥
启用禁用密钥	提供示例介绍如何调用 TCCLI 启用/禁用密钥
密钥轮换	提供示例介绍如何调用 TCCLI 密钥轮换
加密解密	提供示例介绍如何调用 TCCLI 加密解密
删除密钥	提供示例介绍如何调用 TCCLI 删除密钥

创建密钥

最近更新时间：2024-01-11 16:28:53

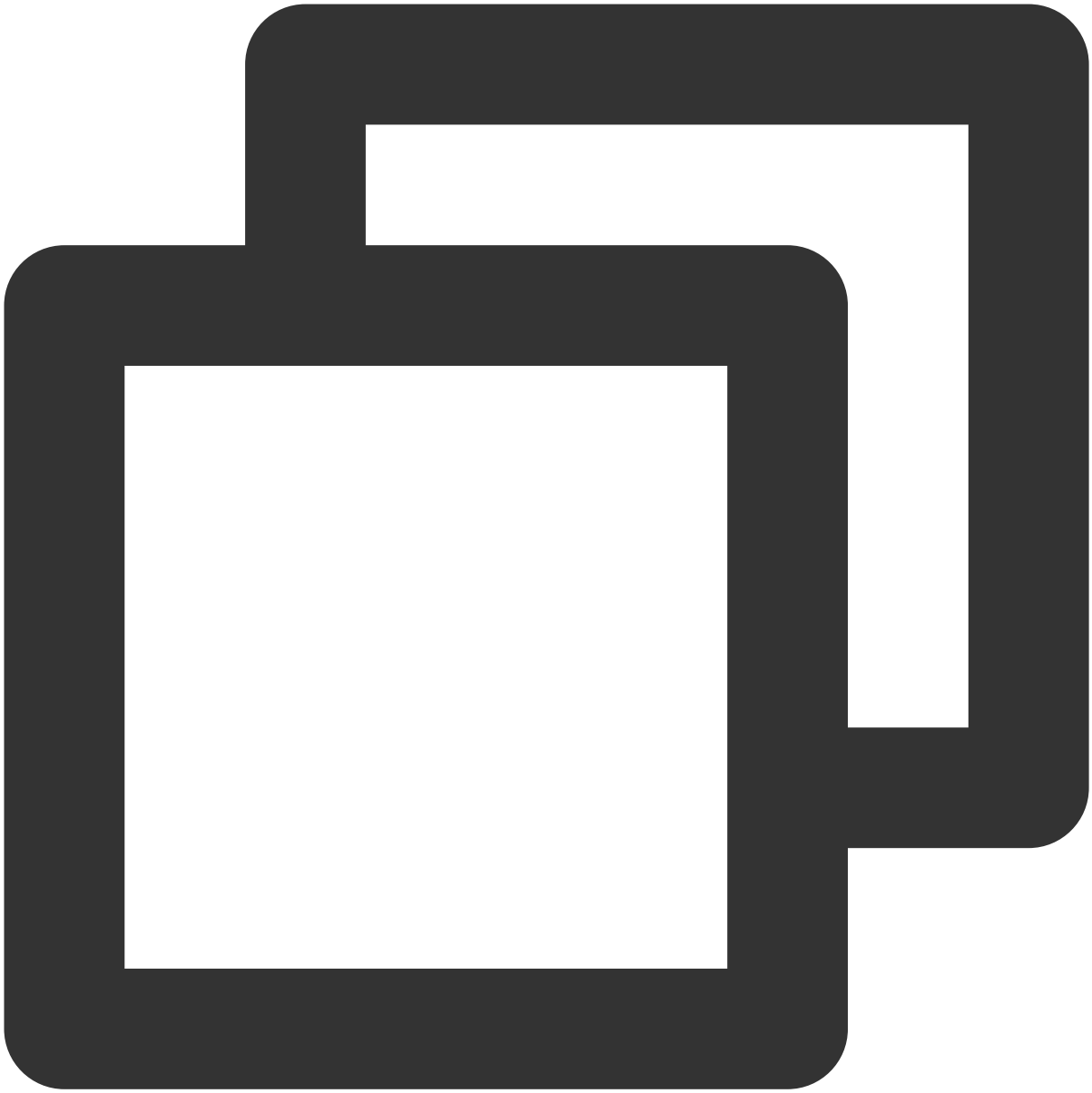
概述

调用 CreateKey 来创建用户管理数据密钥的主密钥 CMK（Custom Master Key），后续可以通过 CMK 来调用其他接口，例如创建数据密钥、加解密等操作。
该 API 操作中的 Alias 为必选参数，您可以查看 CreateKey 接口文档来对 CMK 添加其他描述。
本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

创建一个广州区域，密钥名称为 test-gz01，密钥描述为 this is test for gz key 的 CMK。

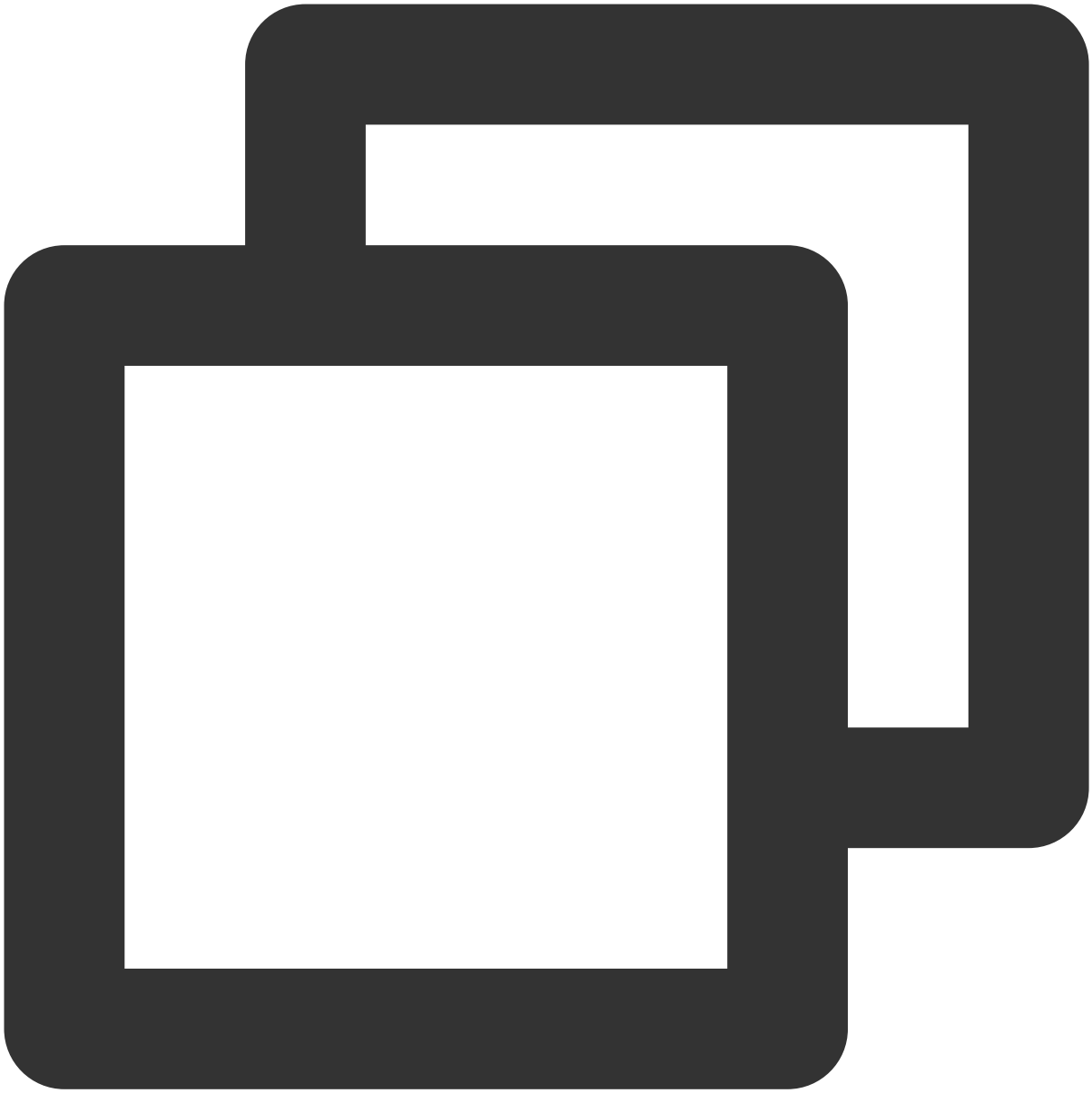
输入



```
tccli kms CreateKey --region ap-guangzhou --Alias test-gz01 --Description 'this is
```

输出

该密钥创建后默认启用，并且默认禁用密钥轮换功能。




```
{
    "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09",
    "Description": "this is test for gz key",
    "Alias": "test-gz01",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "RequestId": "994bbd90-7c8e-4522-85f2-c712da23f863",
    "KeyState": "Enabled",
    "CreateTime": 1571903621
}
```

查看密钥

最近更新时间：2024-01-11 16:28:54

概述

API 名称	API 描述	说明
ListKeys	列出账号下的密钥列表（KeyId 信息）	该 API 操作没有必选参数，详情请参见 ListKeys 接口
DescribeKey	查看指定 CMK 的详细信息，信息包括用户主密钥 CMK 名称、ID、状态、所属地区等密钥详情	该 API 操作的 KeyId 为必选参数，详情请参见 DescribeKey 接口

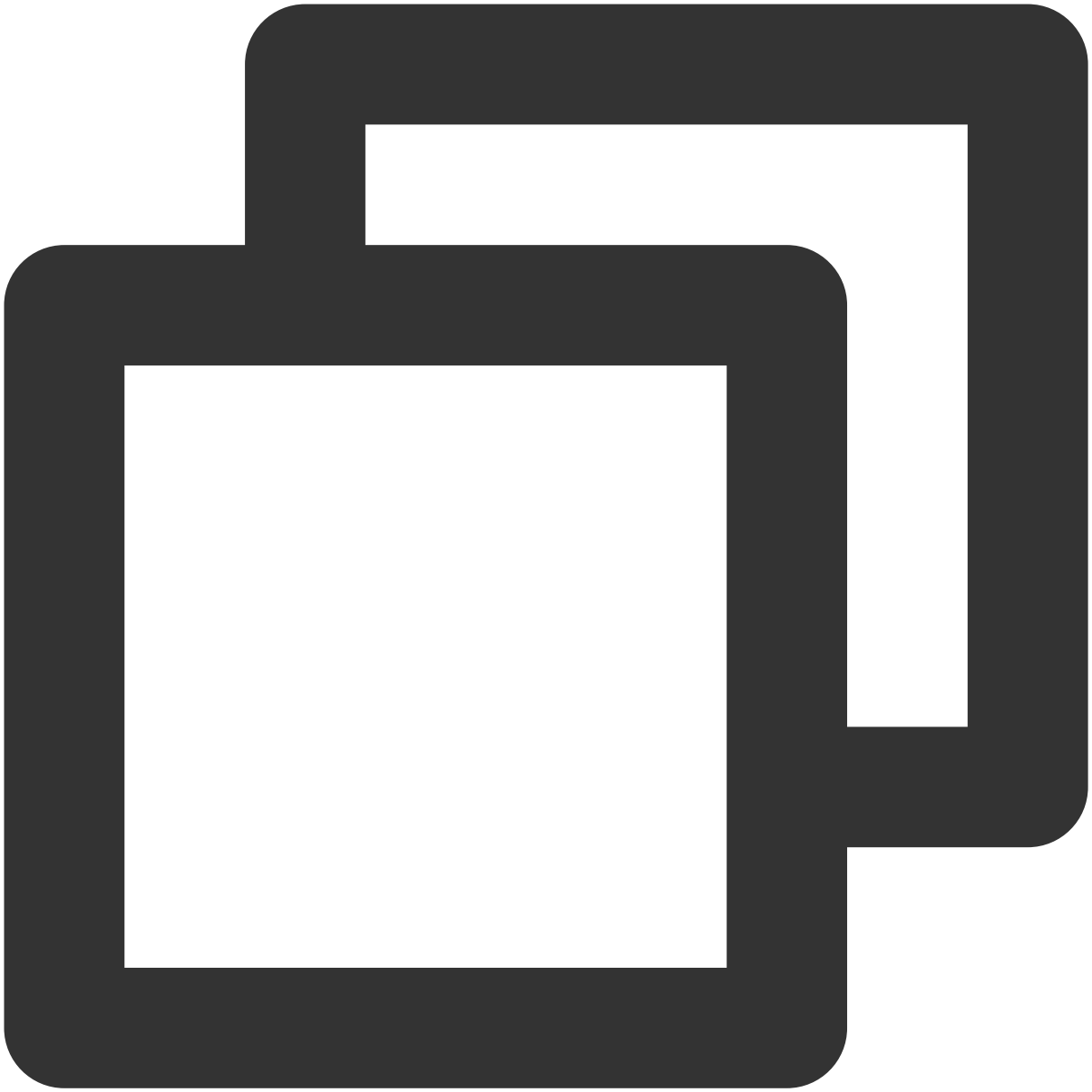
本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

查看密钥 ID 列表示例

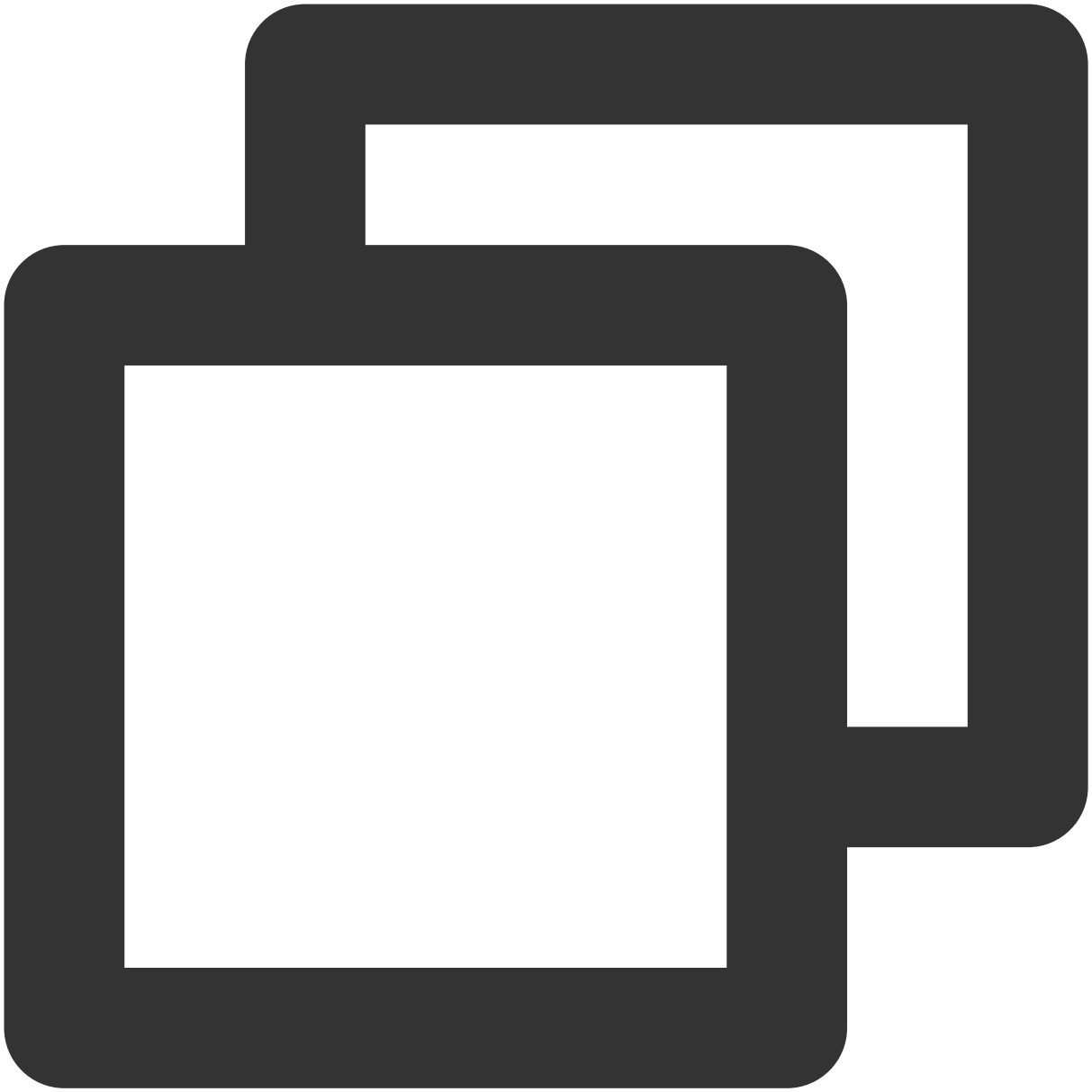
看广东区的前5个 KeyId 信息。

输入



```
tccli kms ListKeys --region ap-guangzhou --Limit 5
```

输出



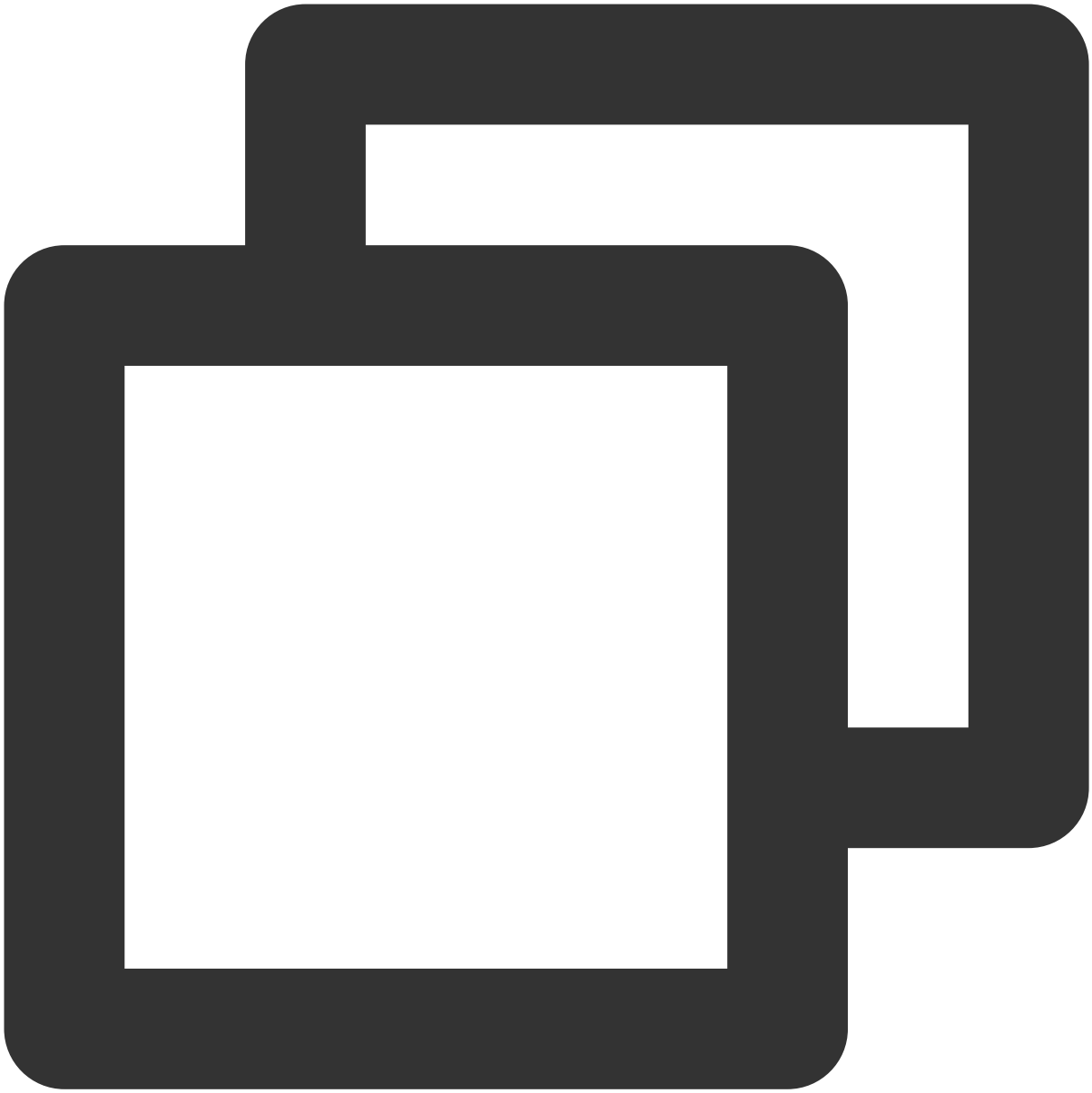

```
{
    "Keys": [
        {
            "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09"
        },
        {
            "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09"
        },
        {
            "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09"
        },
```

```
            {
                "KeyId":"6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09"
            },
            {
                "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09"
            }
        ],
        "TotalCount": 114,
        "RequestId": "afaaeb5e-c97d-4726-8012-6ae337d62928"
    }
```

查看密钥 ID 详情示例

查看指定 CMK 详细信息。

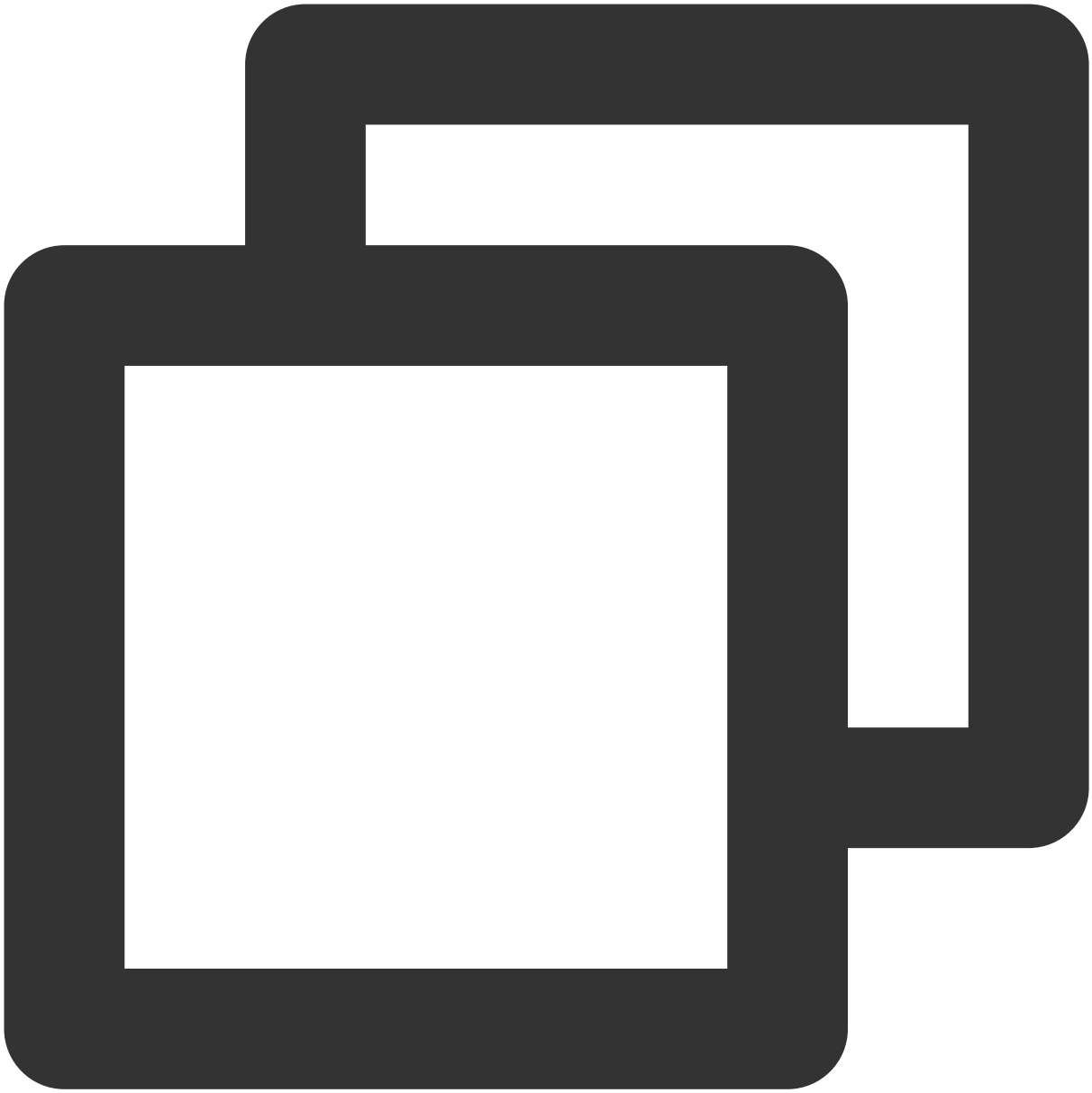
输入



```
tccli kms DescribeKey --region ap-guangzhou --KeyId 521xxxxx-xxxx-xxxx-xxxx-52xxxxd
```

输出

在 API 成功执行的情况下，将返回 CMK 的详细信息。




```
{
 "KeyMetadata": {
        "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09",
        "Description": "this is test for gz key",
        "CreatorUin": 10xxxxxxxxxx,
        "KeyRotationEnabled": false,
        "NextRotateTime": 1603439621,
        "CreateTime": 1571903621,
        "Alias": "test-gz01",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "DeletionDate": 0,
```

```
            "KeyState": "Enabled",
            "Type": 4,
            "Owner": "user"
        },
        "RequestId": "608f514c-3279-44ea-8e4c-c00b69e3521c"
    }
```

编辑密钥

最近更新时间：2024-01-11 16:28:54

概述

修改密钥名称、描述信息操作由两个函数组成，分别如下：

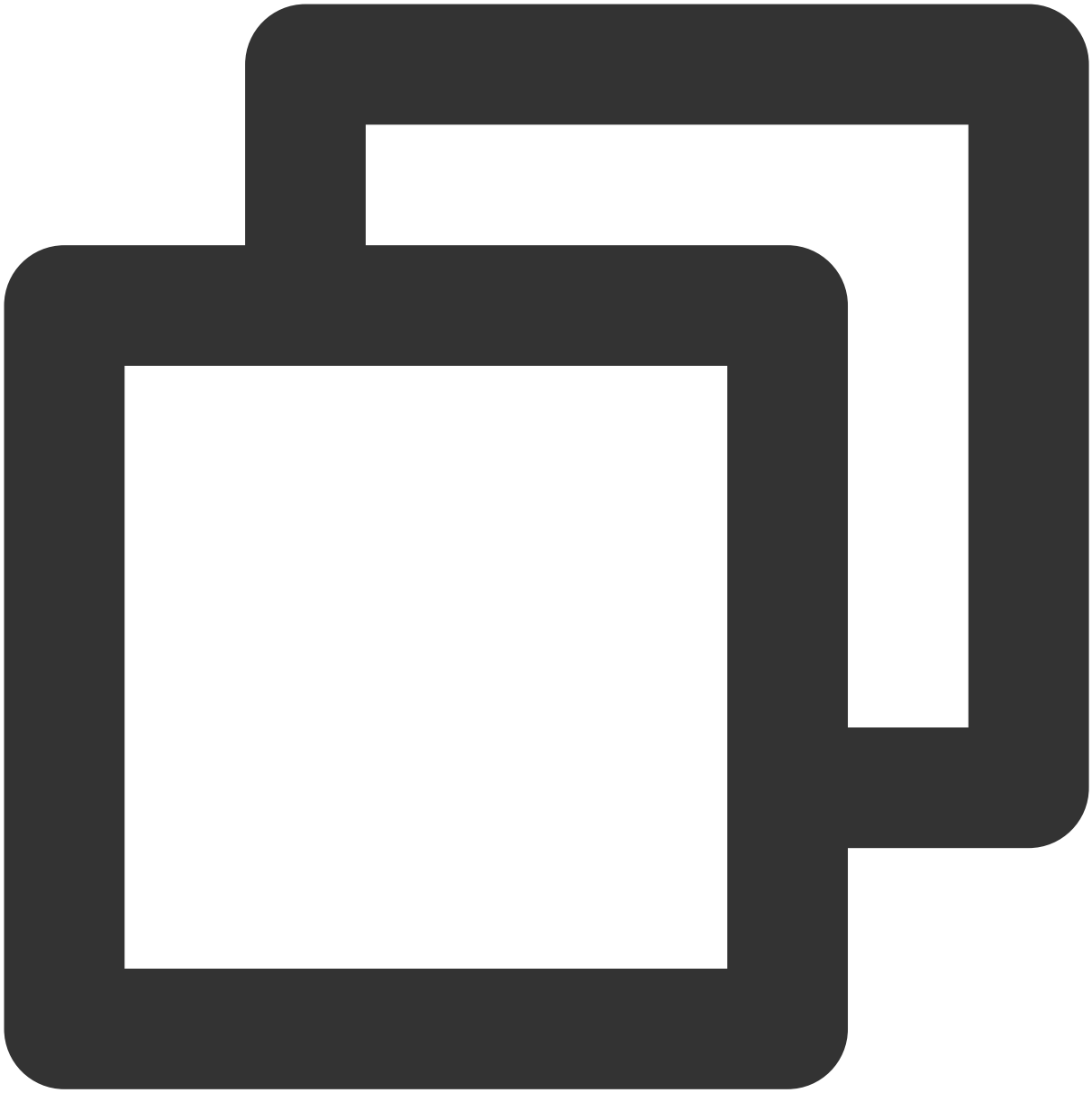
API 名称	API 描述	说明
UpdateAlias	修改密钥名称	该 API 操作的 KeyId 和 Alias 为必选参数，详情请参见 UpdateAlias 接口文档
UpdateKeyDescription	修改密钥描述信息	该 API 操作的 KeyId 和 Description 为必选参数，详情请参见 UpdateKeyDescription 接口文档

本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

修改密钥名称示例

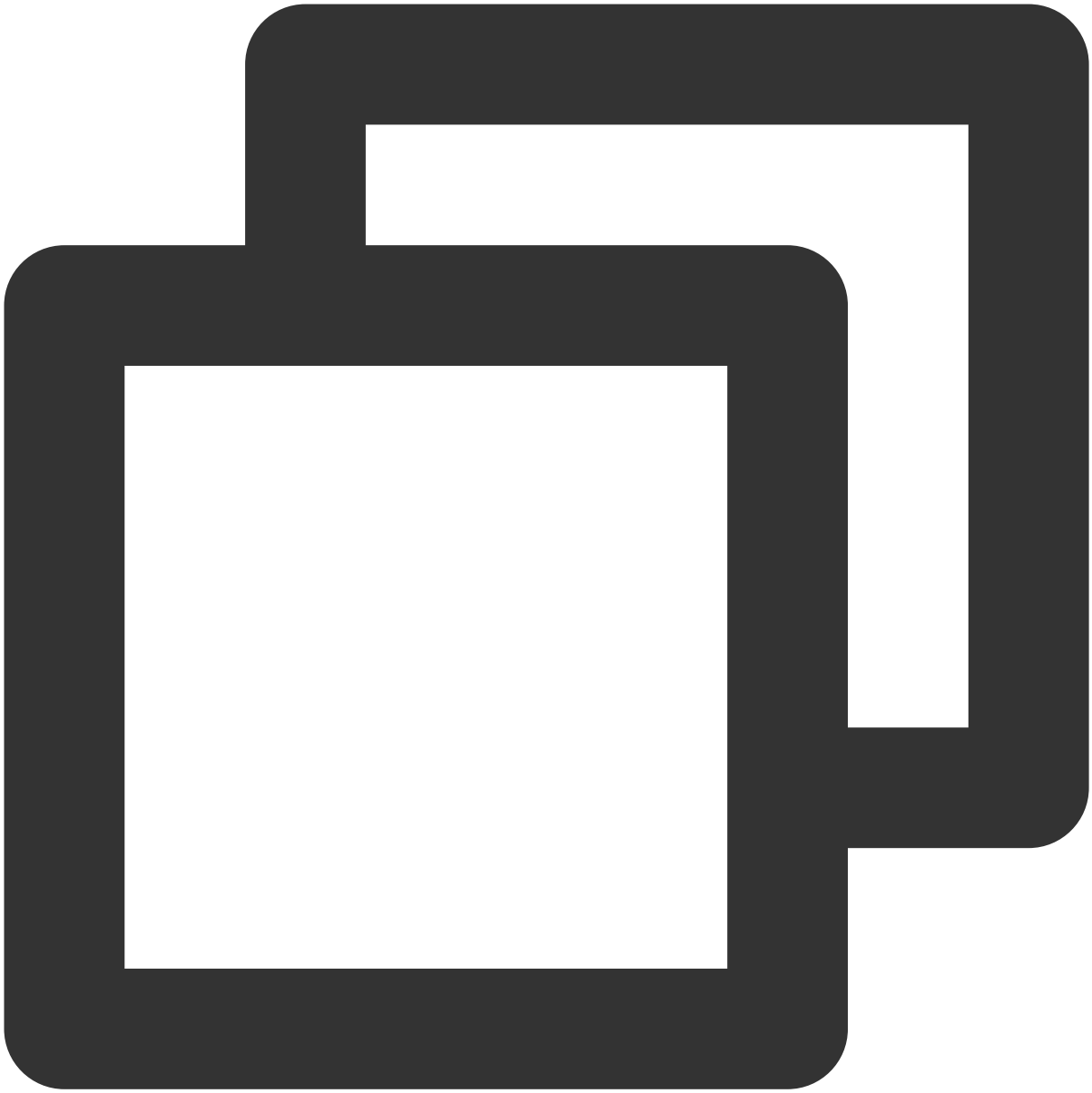
输入



```
tccli kms UpdateAlias --region ap-guangzhou --KeyId 52xxxx-xxxx-xxxx-xxxx-5xxxx4 --
```

输出

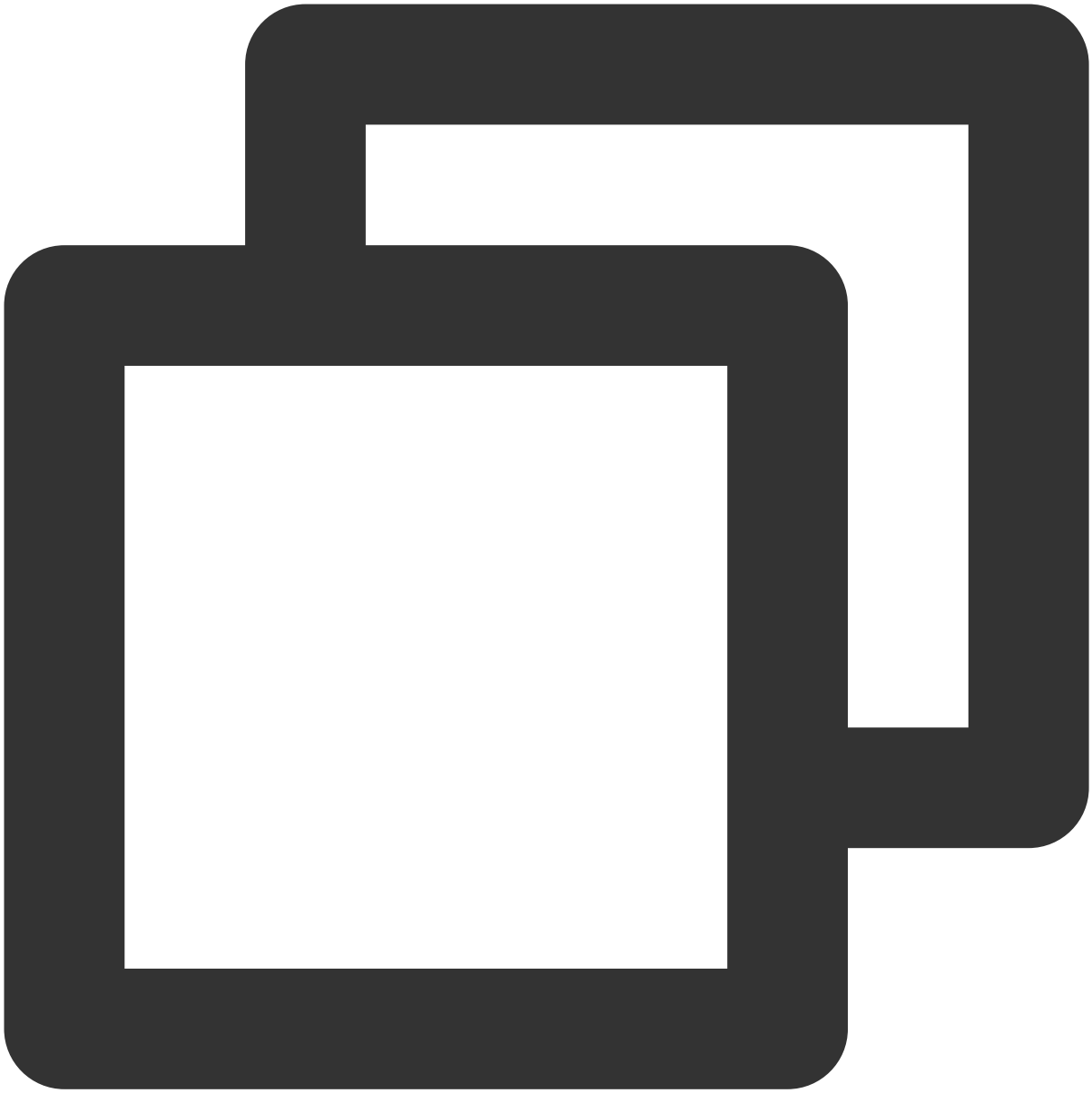
如修改成功将返回如下相关信息。



```
{
    "RequestId": "489a4274-0b81-4db7-8160-542c5c5bed68"
}
```

修改密钥描述信息示例

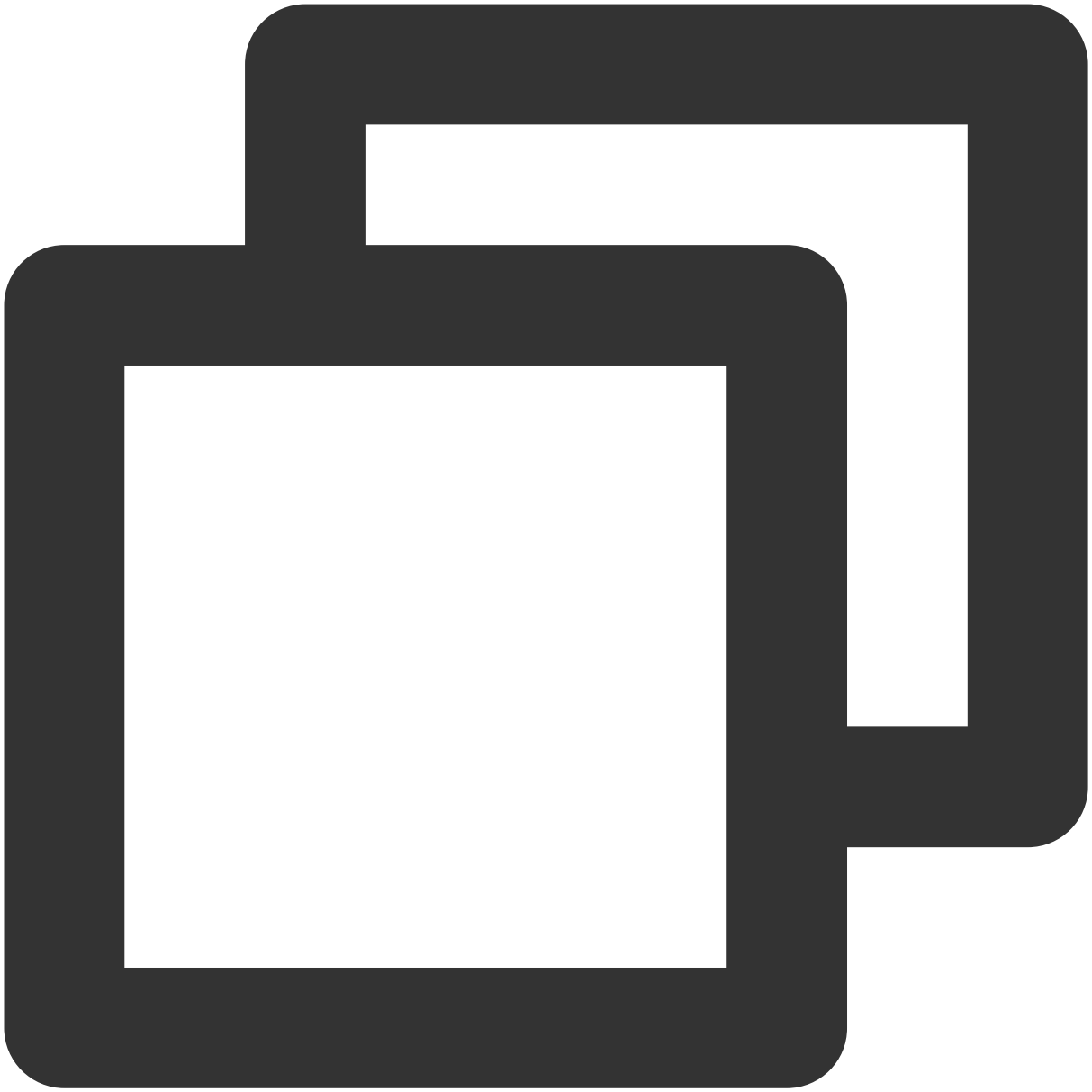
输入



```
tccli kms UpdateKeyDescription --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-
```

输出

如修改成功将返回如下相关信息。



```
{
    "RequestId": "31134207-5de8-44f2-8c00-8bd0e88f95a6"
}
```

启用禁用密钥

最近更新时间：2024-01-11 16:28:54

概述

密钥启用/禁用 API 操作由两个函数组成，分别如下：

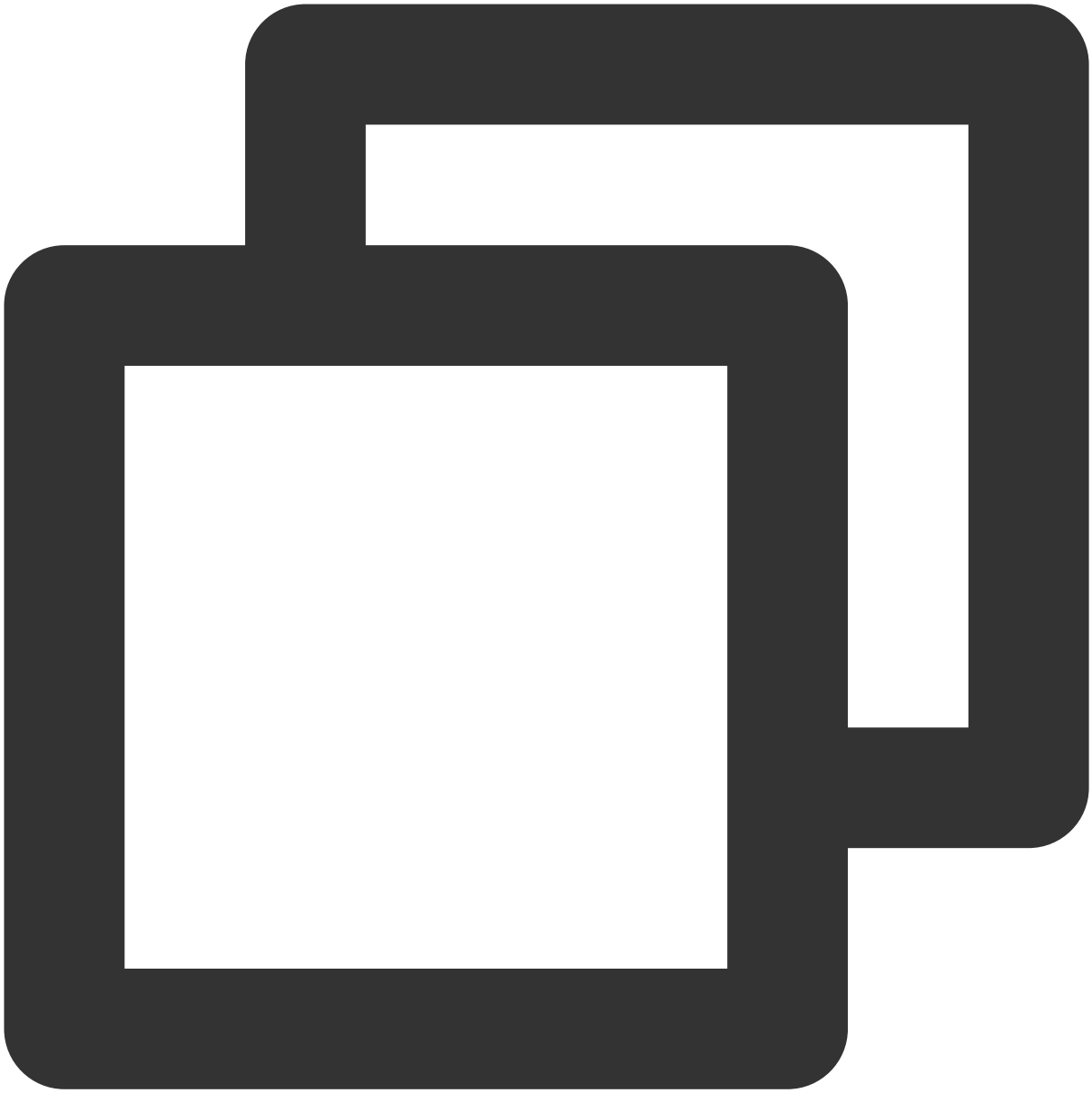
API 名称	API 描述	说明
EnableKey	启用主密钥	该 API 操作的 KeyId 为必选参数，详情请参见 EnableKey 接口文档
DisableKey	禁用主密钥	该 API 操作的 KeyId 为必选参数，详情请参见 DisableKey 接口文档

本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

启用密钥示例

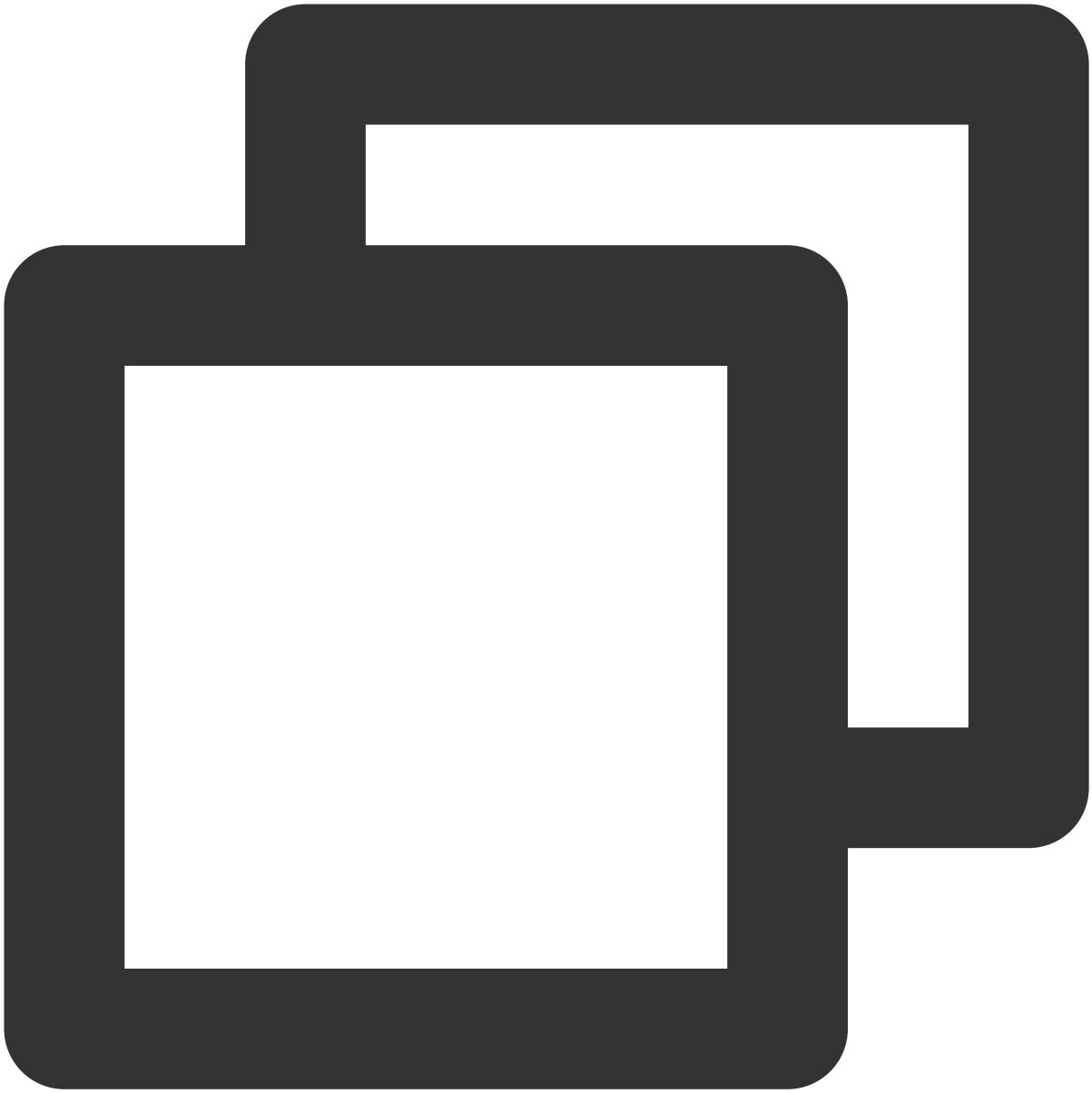
输入



```
tccli kms EnableKey --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-52xxxxx4
```

输出

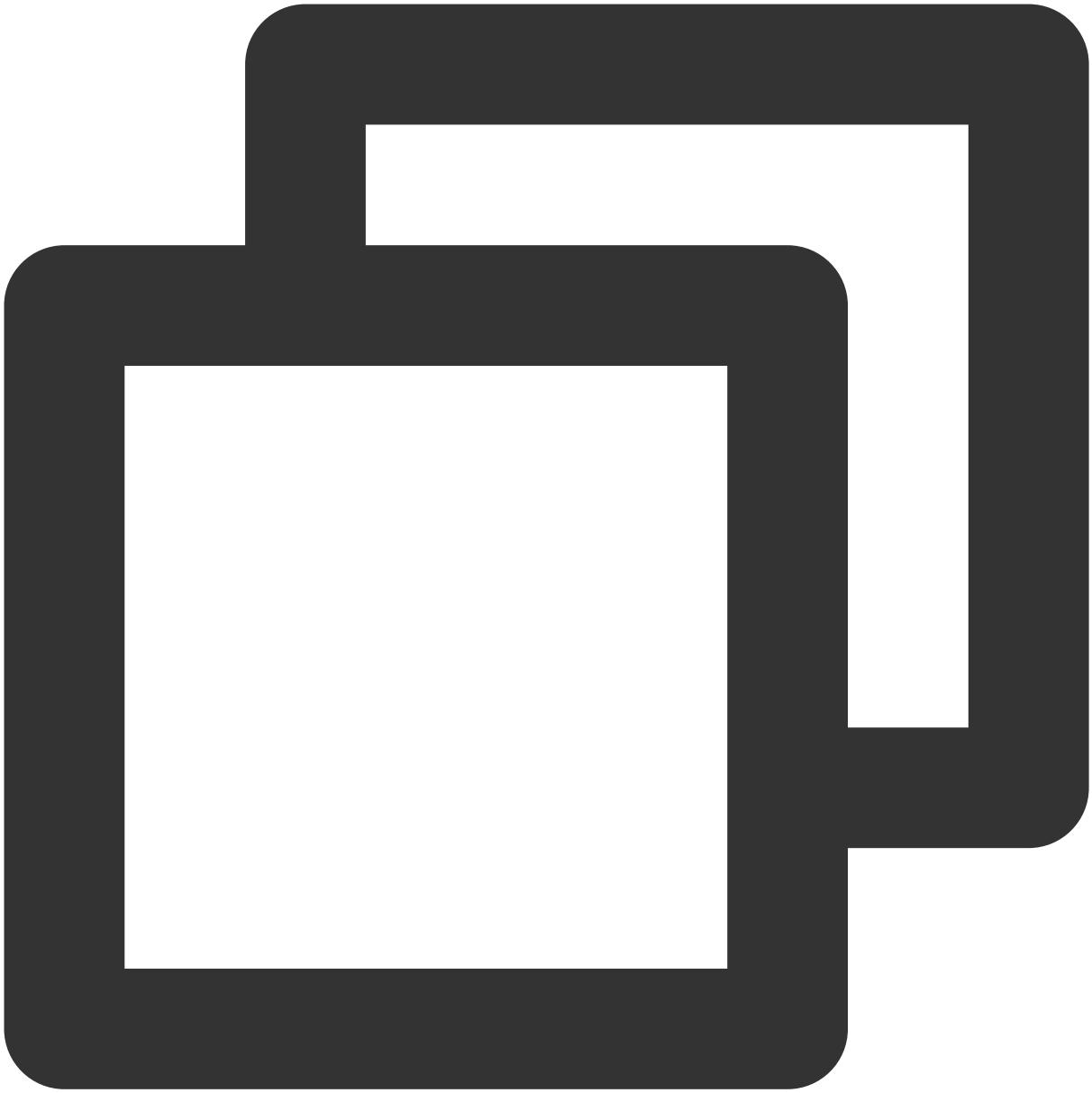
如成功启用密钥，将返回如下请求。



```
{
    "RequestId": "6b2187b0-f40a-46d0-8065-2434afc54619"
}
```

禁用密钥示例

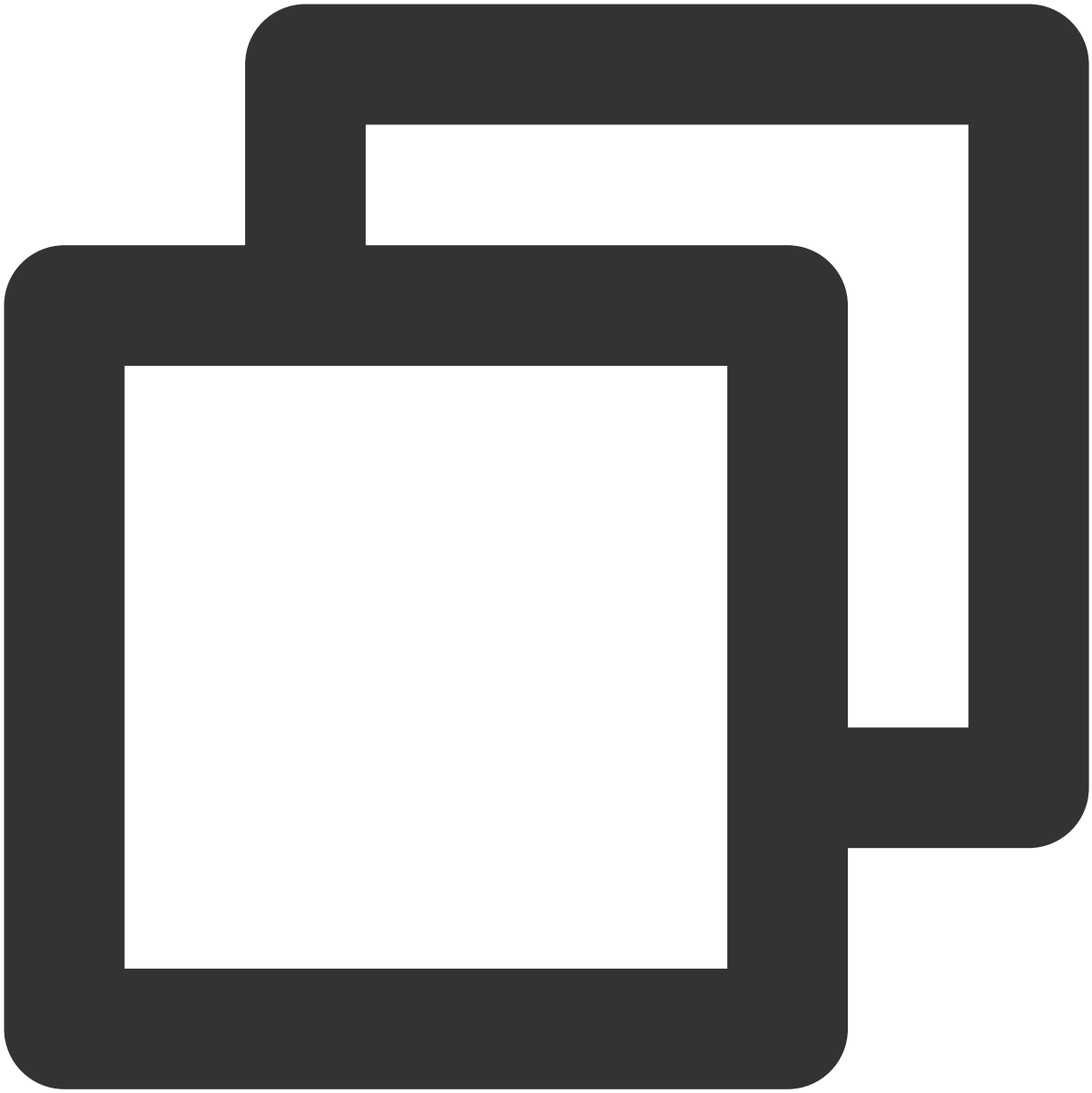
输入



```
tccli kms DisableKey --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-52xxxxx4
```

输出

如成功禁用密钥，将返回如下请求。



```
{
    "RequestId": "e5674638-1466-4607-a3ea-b60d30f4e5e3"
}
```

密钥轮换

最近更新时间：2024-01-11 16:28:54

概述

密钥轮换功能操作分三个API组成，分别如下：

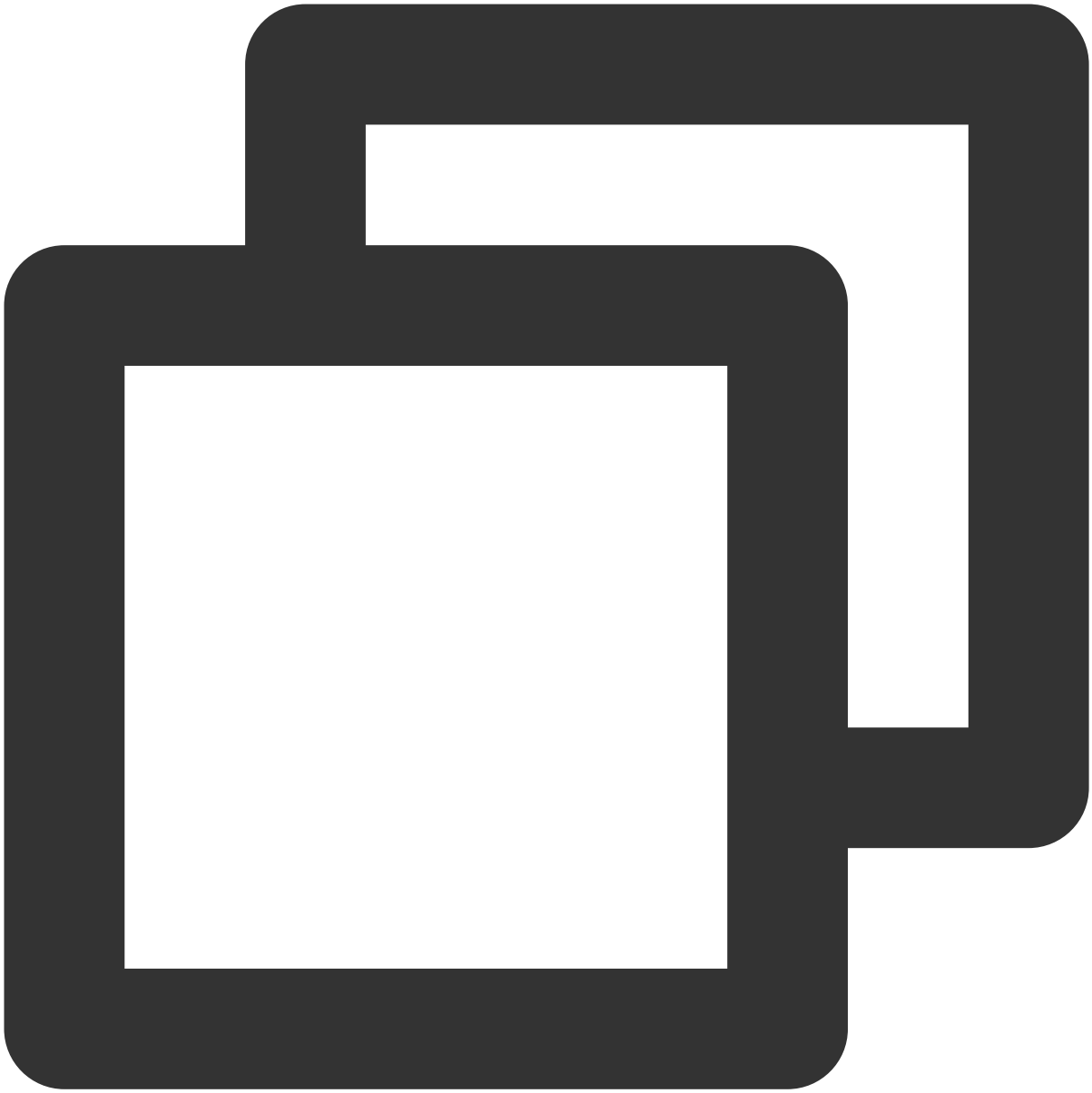
API 名称	API 描述	说明
GetKeyRotationStatus	查看密钥轮换功能状态	该 API 操作的 KeyId 为必选参数，详情请参见 GetKeyRotationStatus 接口文档
EnableKeyRotation	开启密钥轮换	该 API 操作的 KeyId 为必选参数，详情请参见 EnableKeyRotation 接口文档
DisableKeyRotation	禁止密钥轮换	该 API 操作的 KeyId 为必选参数，详情请参见 DisableKeyRotation 接口文档

本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

查看密钥轮换状态示例

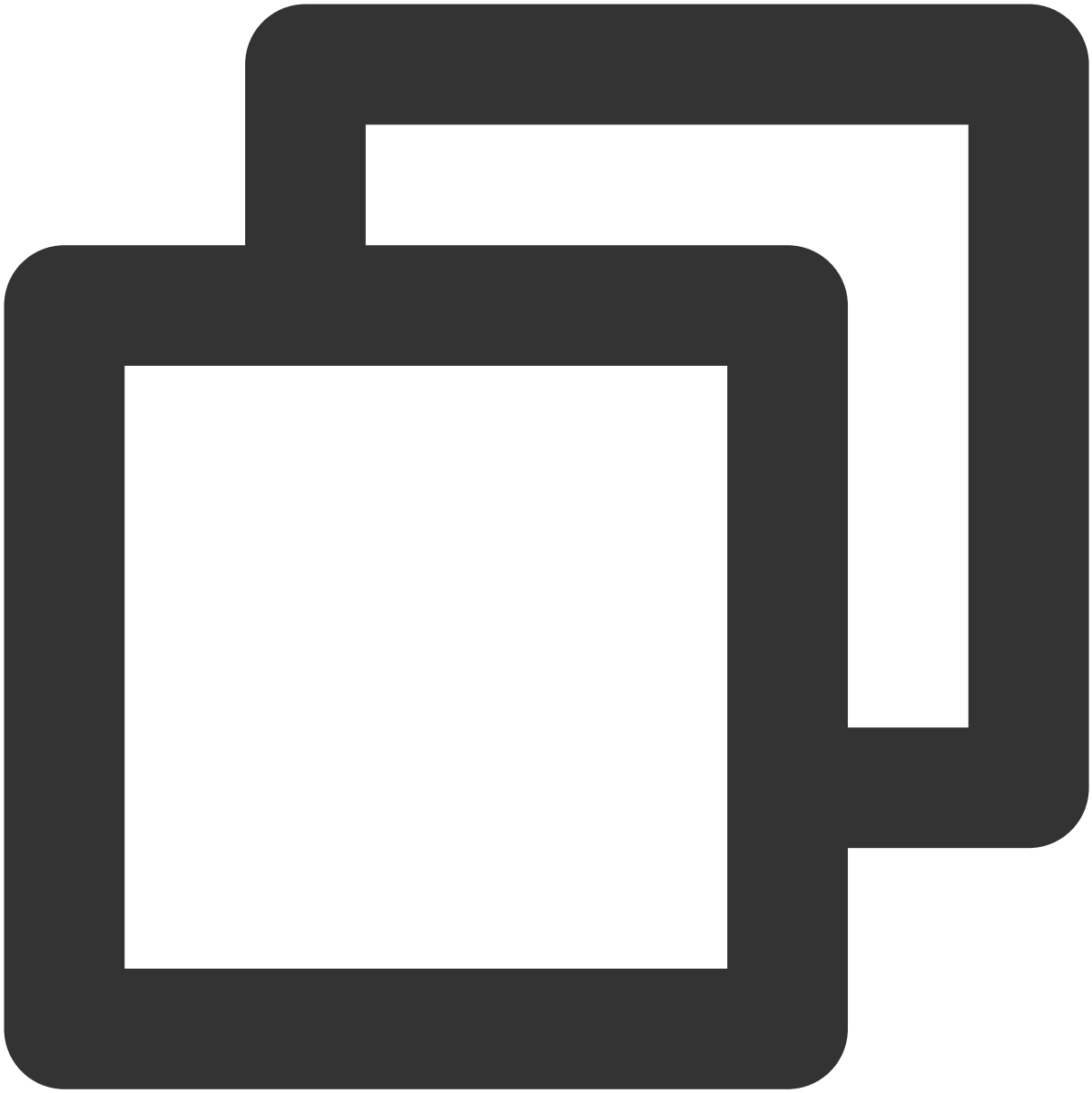
输入



```
tccli kms GetKeyRotationStatus --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-
```

输出

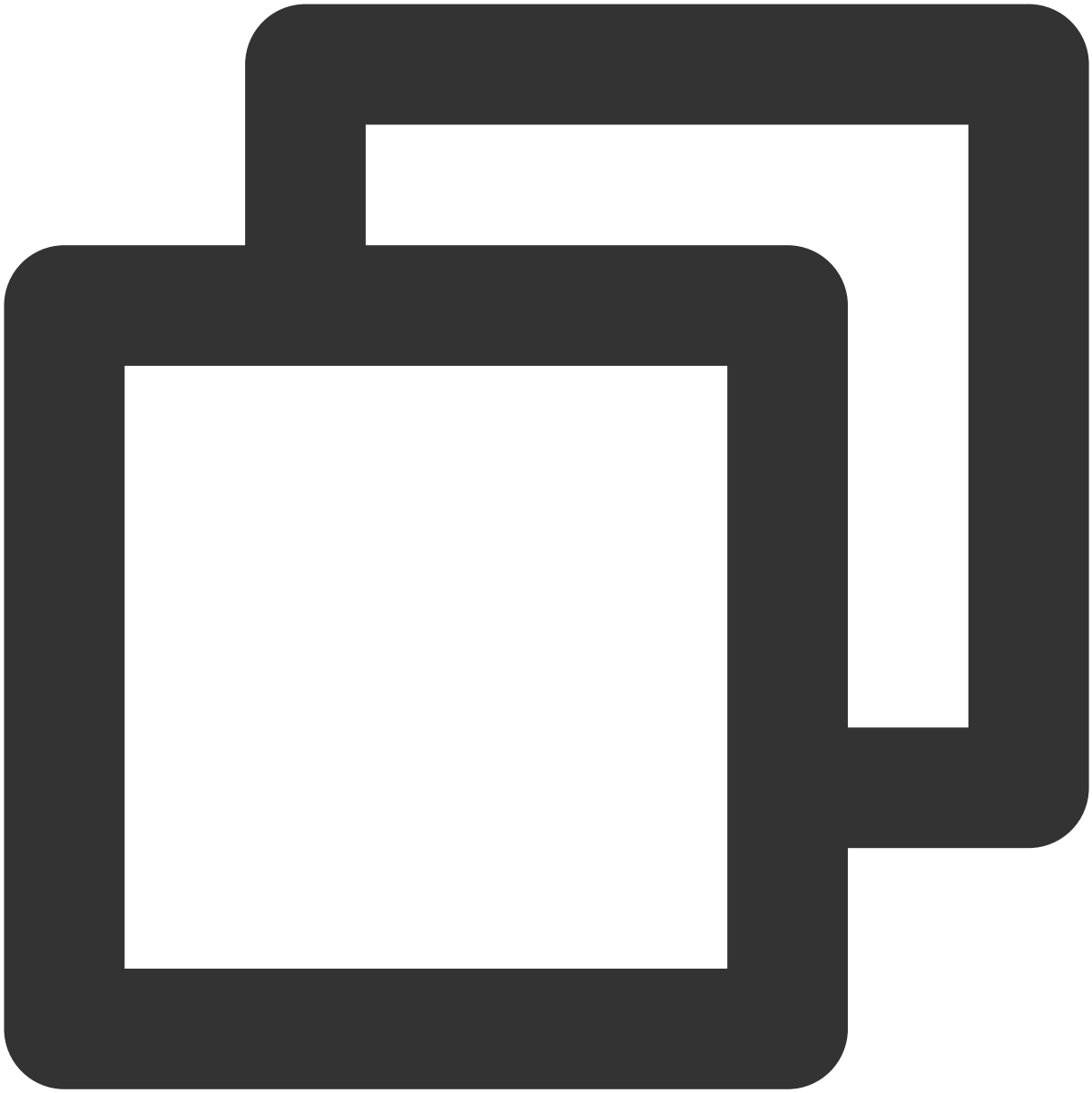
在 API 成功调用时，将返回 CMK 的密钥轮换状态。



```
{
    "KeyRotationEnabled": false,
    "RequestId": "e1432224-4dc2-48da-a8e8-e84d30afd9ef"
}
```

开启密钥轮换示例

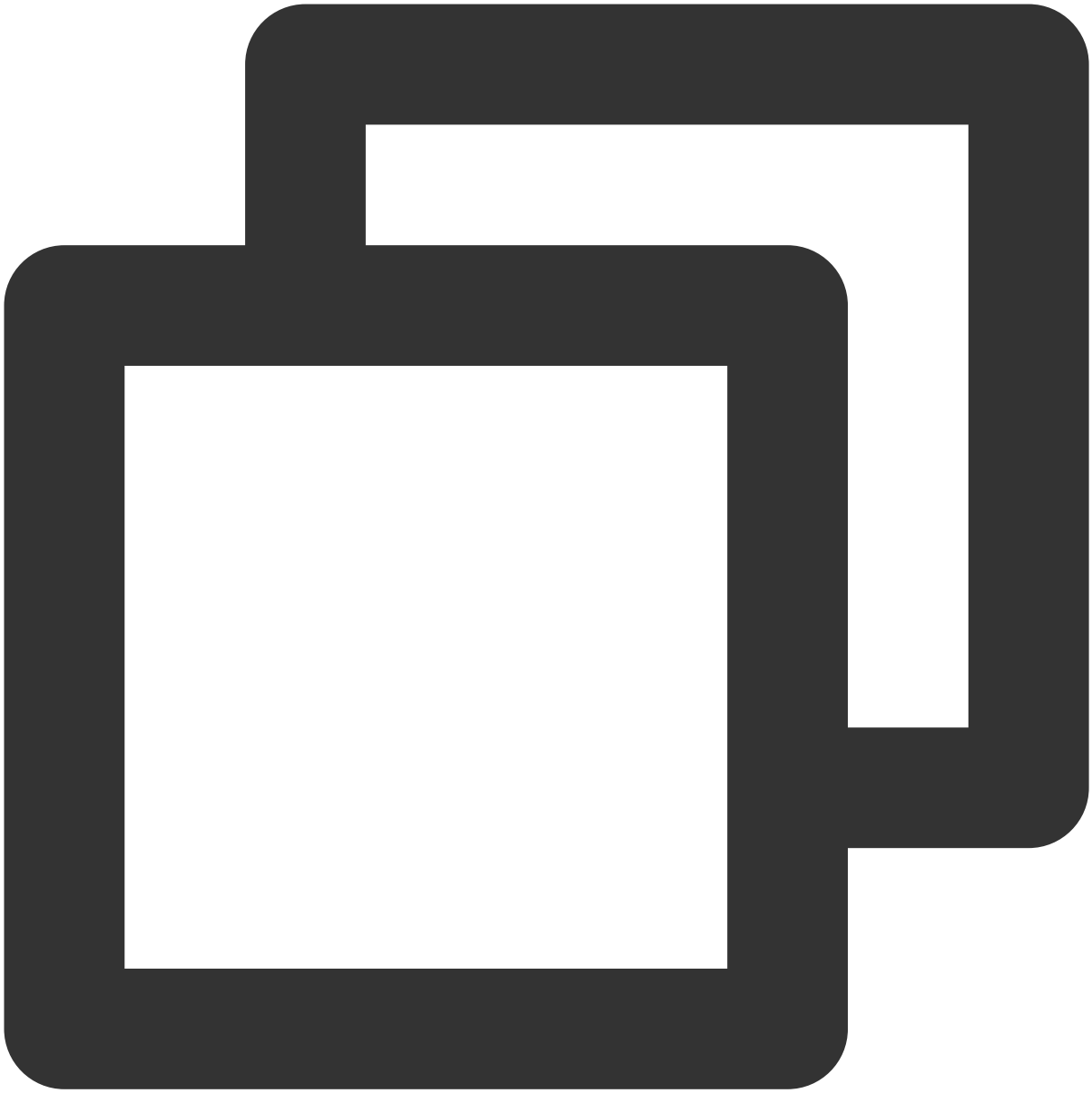
输入



```
tccli kms EnableKeyRotation --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-52x
```

输出

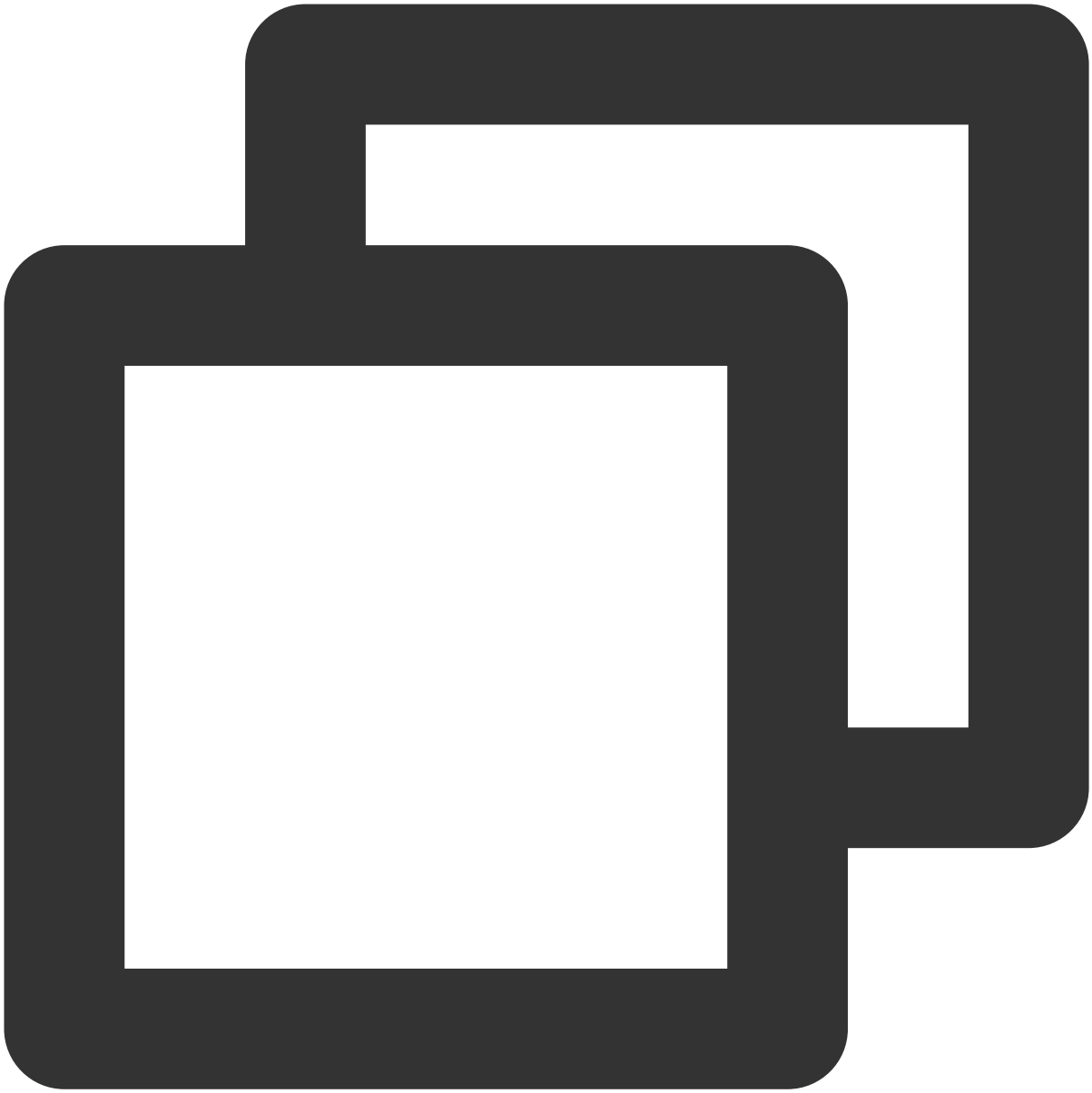
如正常开启该功能，将返回如下请求信息。



```
{
    "RequestId": "4e0fa96f-e86e-4517-af27-3dfe6e5b2a72"
}
```

禁止密钥轮换示例

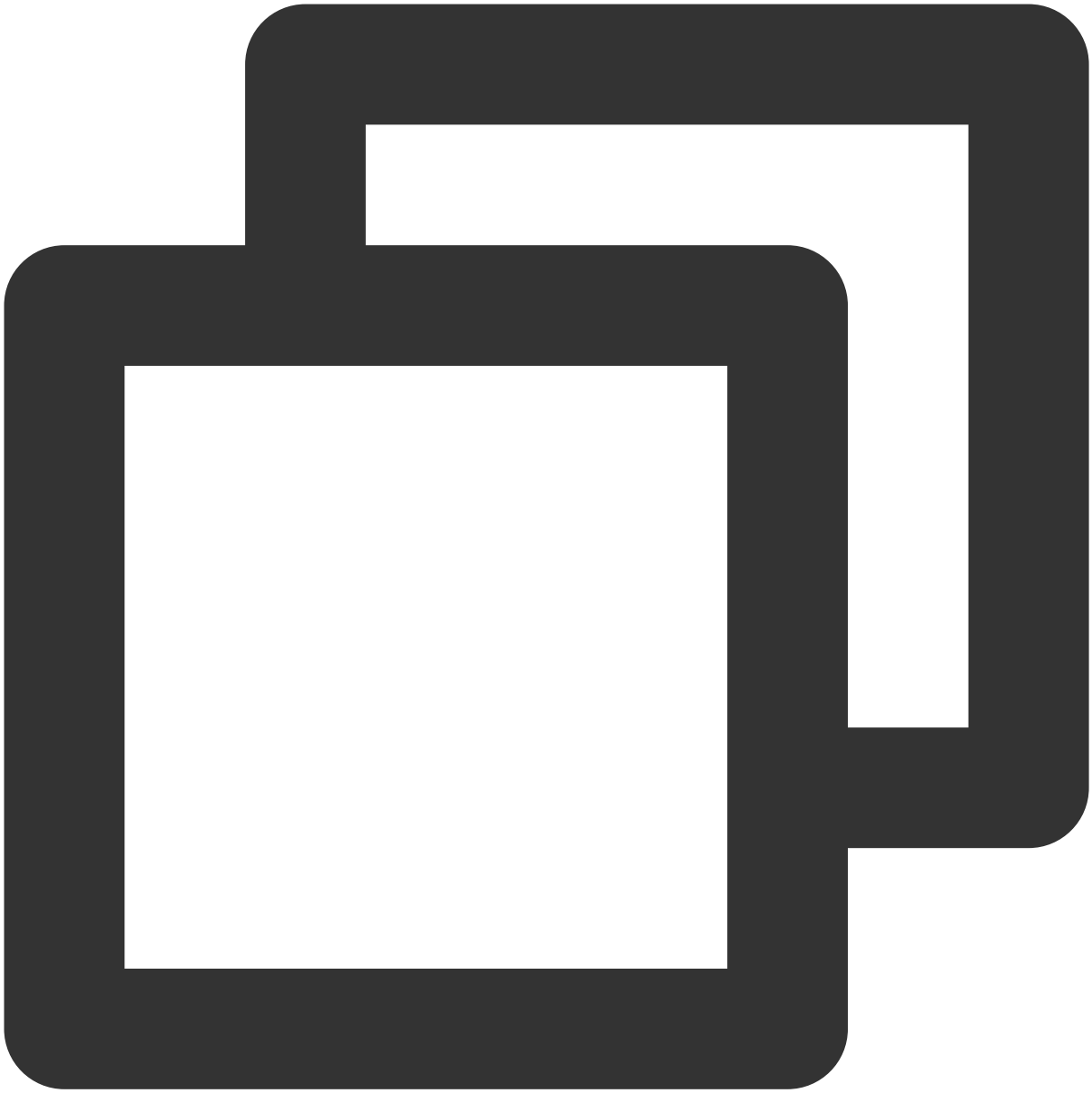
输入



```
tccli kms DisableKeyRotation --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-52
```

输出

如正常开启该功能，将返回如下请求信息。



```
{
    "RequestId": "c8b73c8b-1ee5-4b23-b800-7cccc58e7ffb"
}
```

对称密钥加解密

最近更新时间：2024-01-11 16:28:54

概述

在线加密解密功能操作分两个 API 组成，分别如下：

API 名称	API 描述	说明
Encrypt	加密	该 API 操作的 KeyId 和 Plaintext 为必选参数，详情请参见 Encrypt 接口文档
Decrypt	解密	该 API 操作的 CiphertextBlob 为必选参数，详情请参见 Decrypt 接口文档

加密

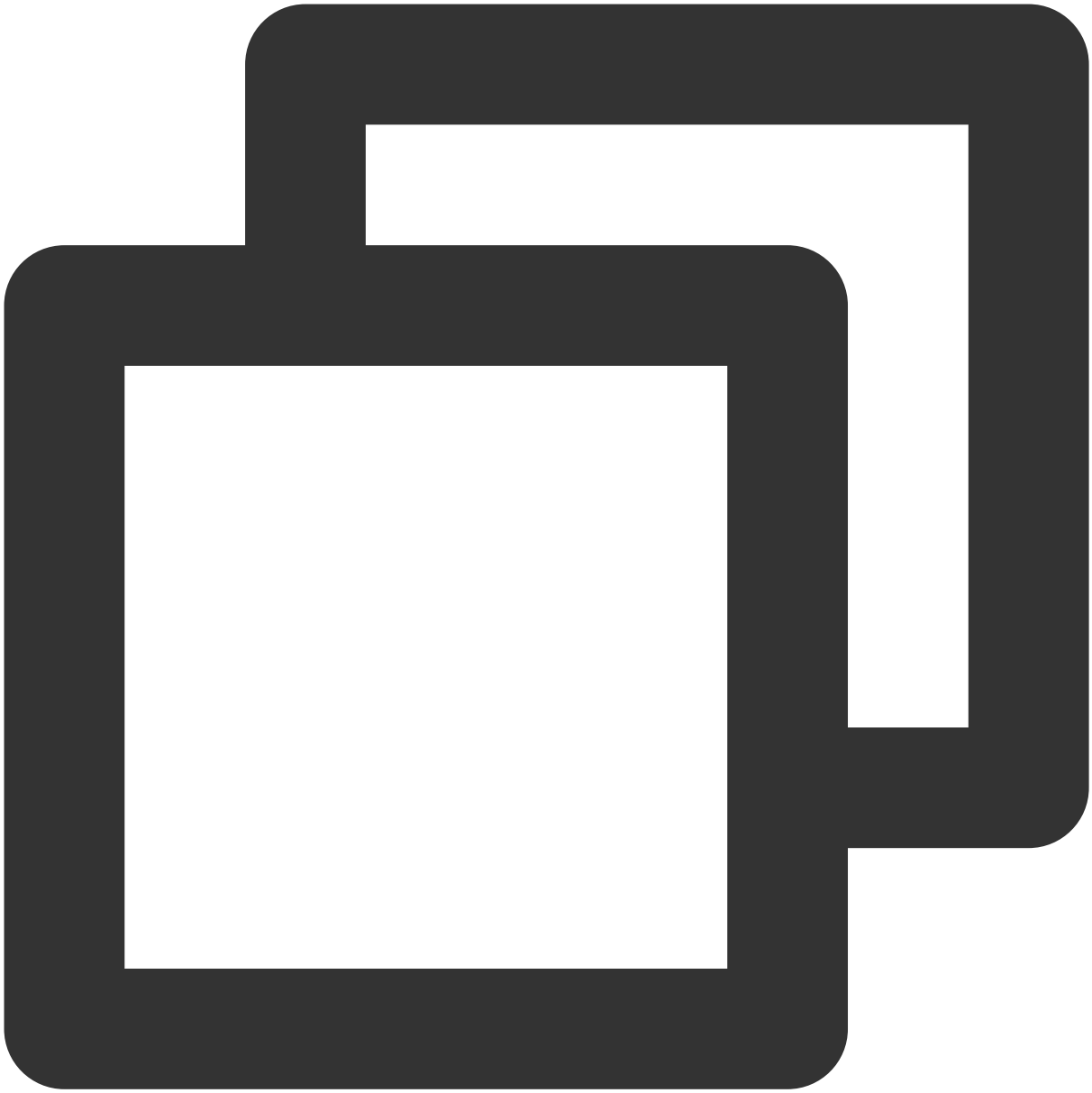
通过 Encrypt 来针对用户的数据进行加密，用于加密的数据大小最多为4KB任意数据，可用于加密数据库密码，RSA Key，或其它较小的敏感信息。对于应用的数据加密，推荐使用 GenerateDataKey 生成的 DEK 进行本地数据的加解密操作。
本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

加密示例

使用 TCCLI 调用加密接口时，需对明文数据进行 Base64 编码。本案例使用 This example is used for testing 文本案例。

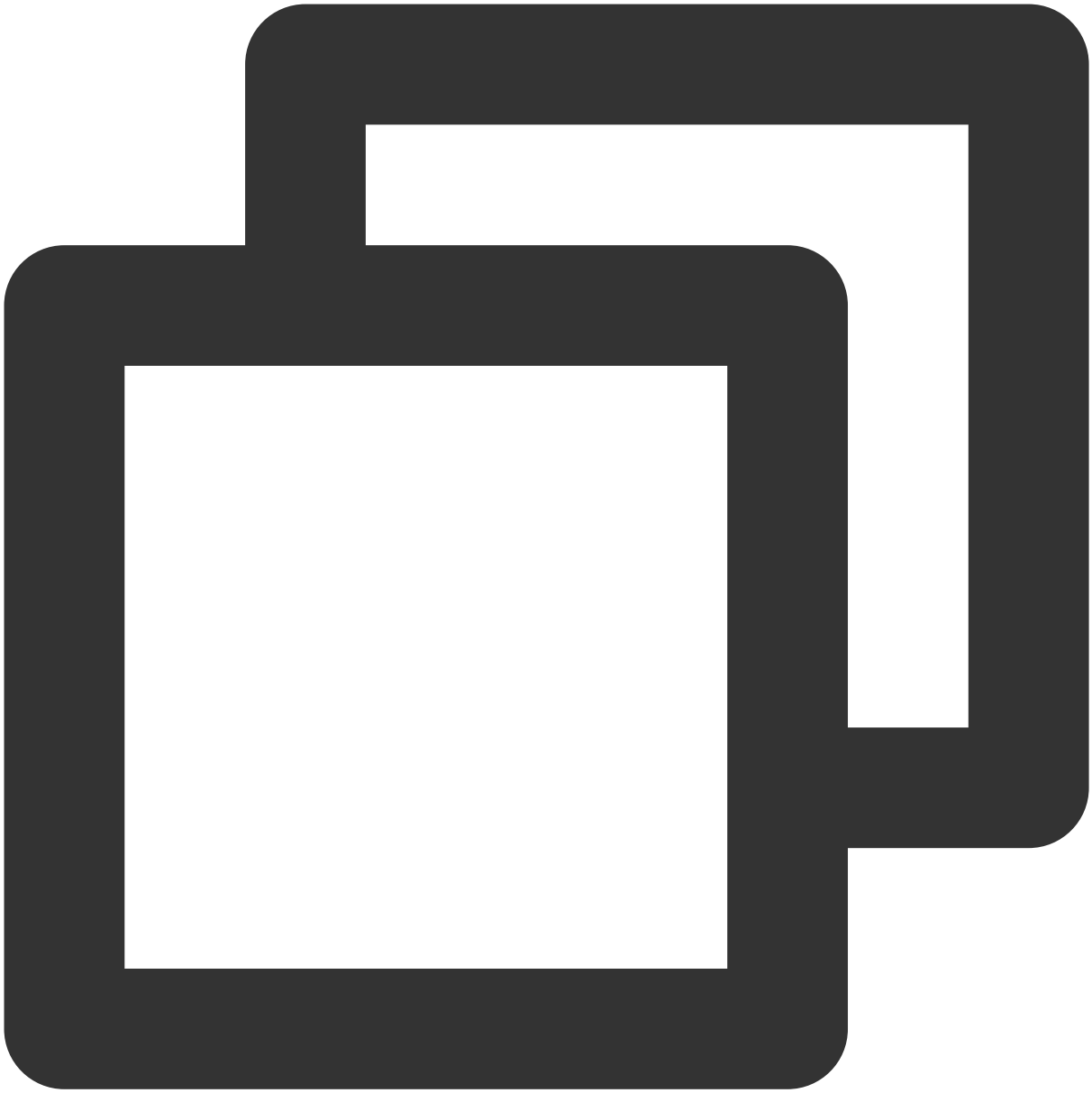
输入



```
tccli kms Encrypt --KeyId 6xxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxx5 --Plaintext "VGhpcyBle
```

输出

如成功执行，请求数据将返回密文和加密该明文的 CMK ID，其中密文将用来后续的解密操作。

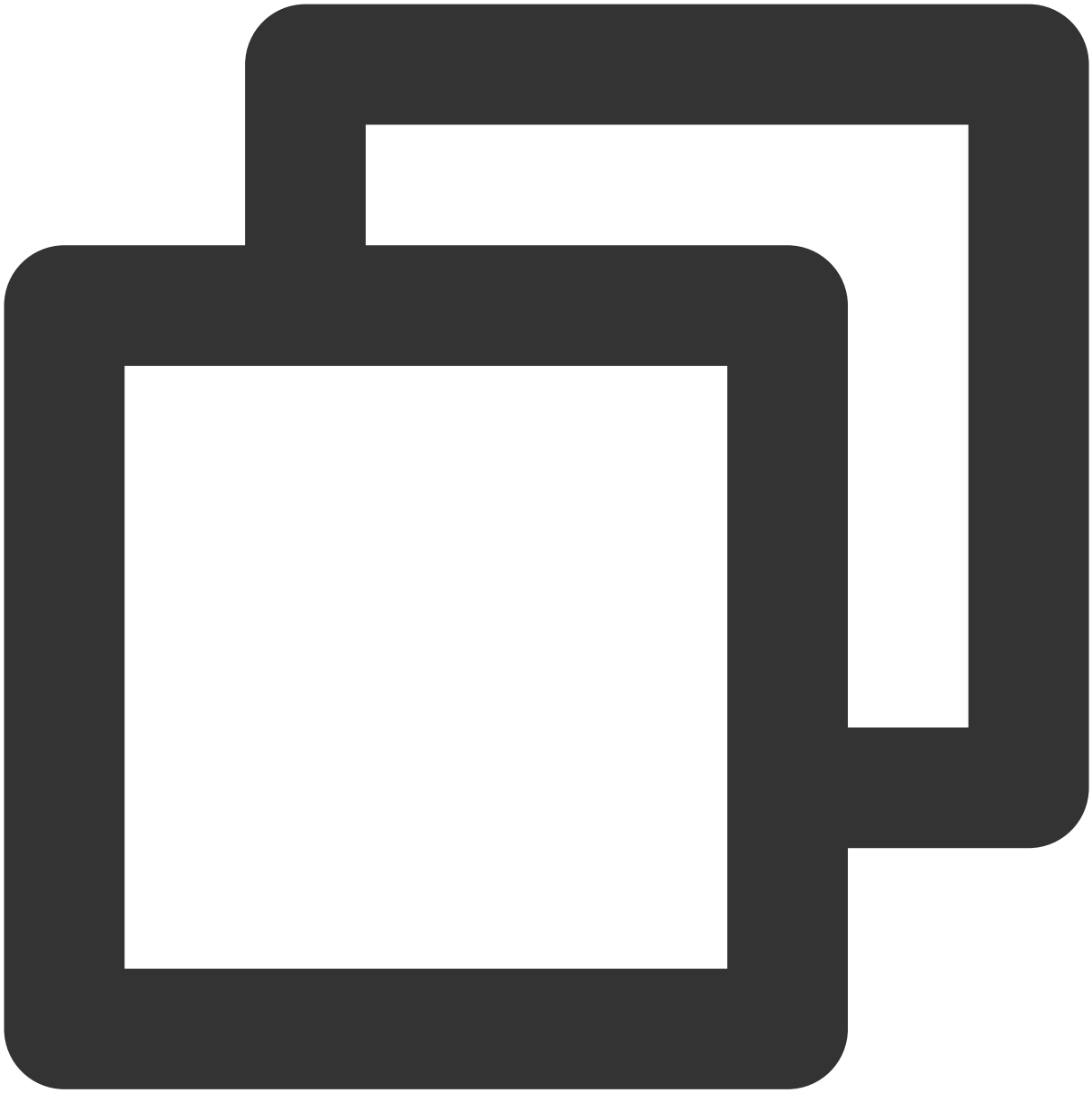


```
{
    "KeyId": "6xxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxx5",
    "RequestId": "23781471-c213-44c5-92a4-731b882e25b5",
    "CiphertextBlob": "RrnqzfthTxcSdCYIw5pBoEWLvrdqYNZ0oXKOmvYx/1Oo2R+DqEFPjjfVA1n
}
```

解密示例

现在我们来针对加密数据进行解密。其中示例流程中的 CMK 以上述创建的 CMK 为例。

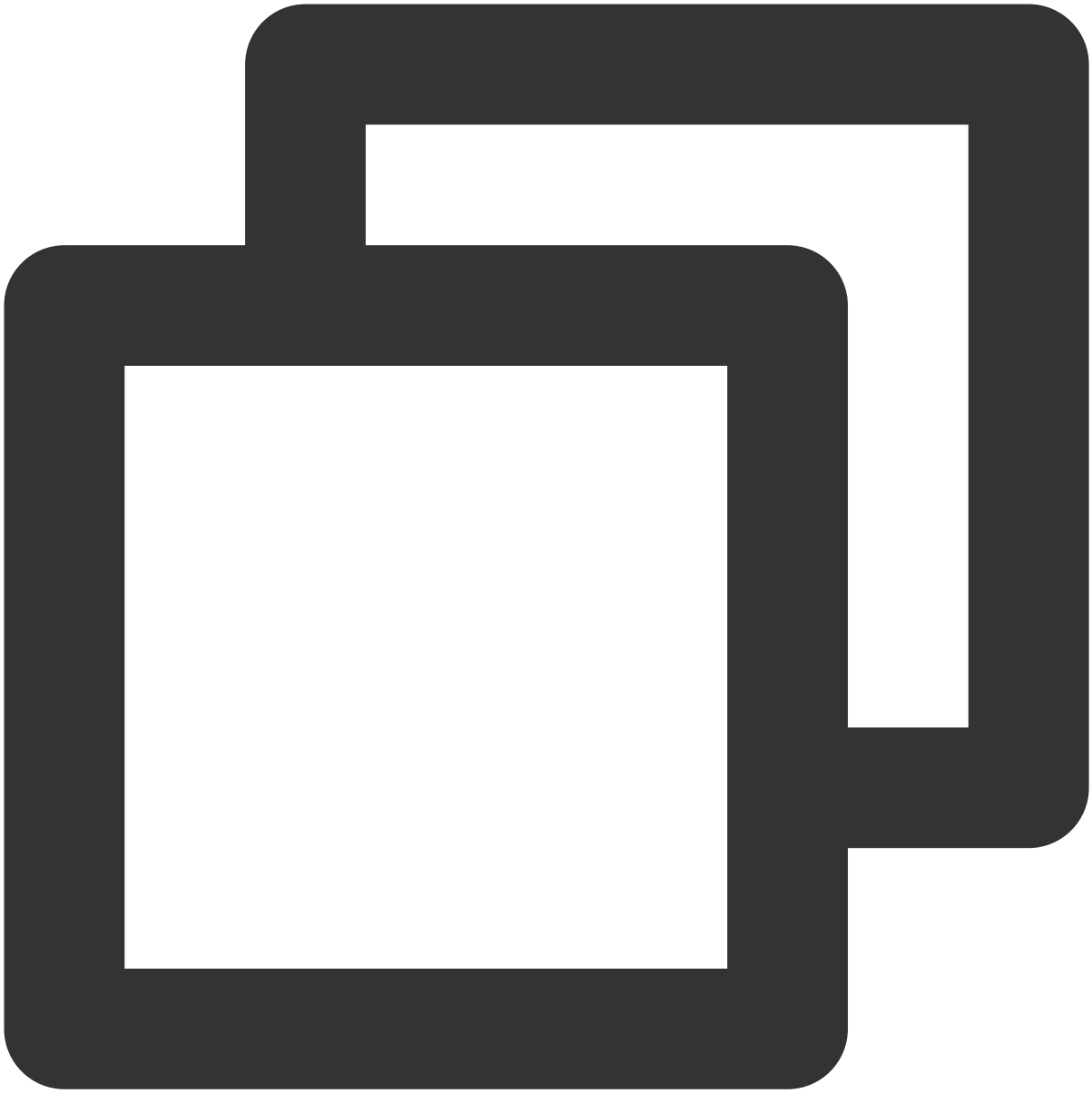
输入



```
tccli kms Decrypt --CiphertextBlob "Rrnqz5fthTxcSdCYIw5pBoEWLvrdqYNZ0oXKOmvYx/1Oo2R
```

输出

如成功执行，请求数据将返回 Base64 编码的明文和加密该明文的 CMK ID。后续需要进行额外的 Base64 解密操作获取明文。




```
{
    "Plaintext": "VGhpcyBleGFtcGxlIGlzIHVzZWQgZm9yIHRlc3Rpbmc=",
    "KeyId": "6xxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxx5",
    "RequestId": "bcce3fae-1794-4136-a486-d42780c10702"
}
```

非对称密钥解密

最近更新时间：2024-01-11 16:28:54

概述

KMS 提供 SM2 和 RSA 的非对称密钥解密接口，分别如下：

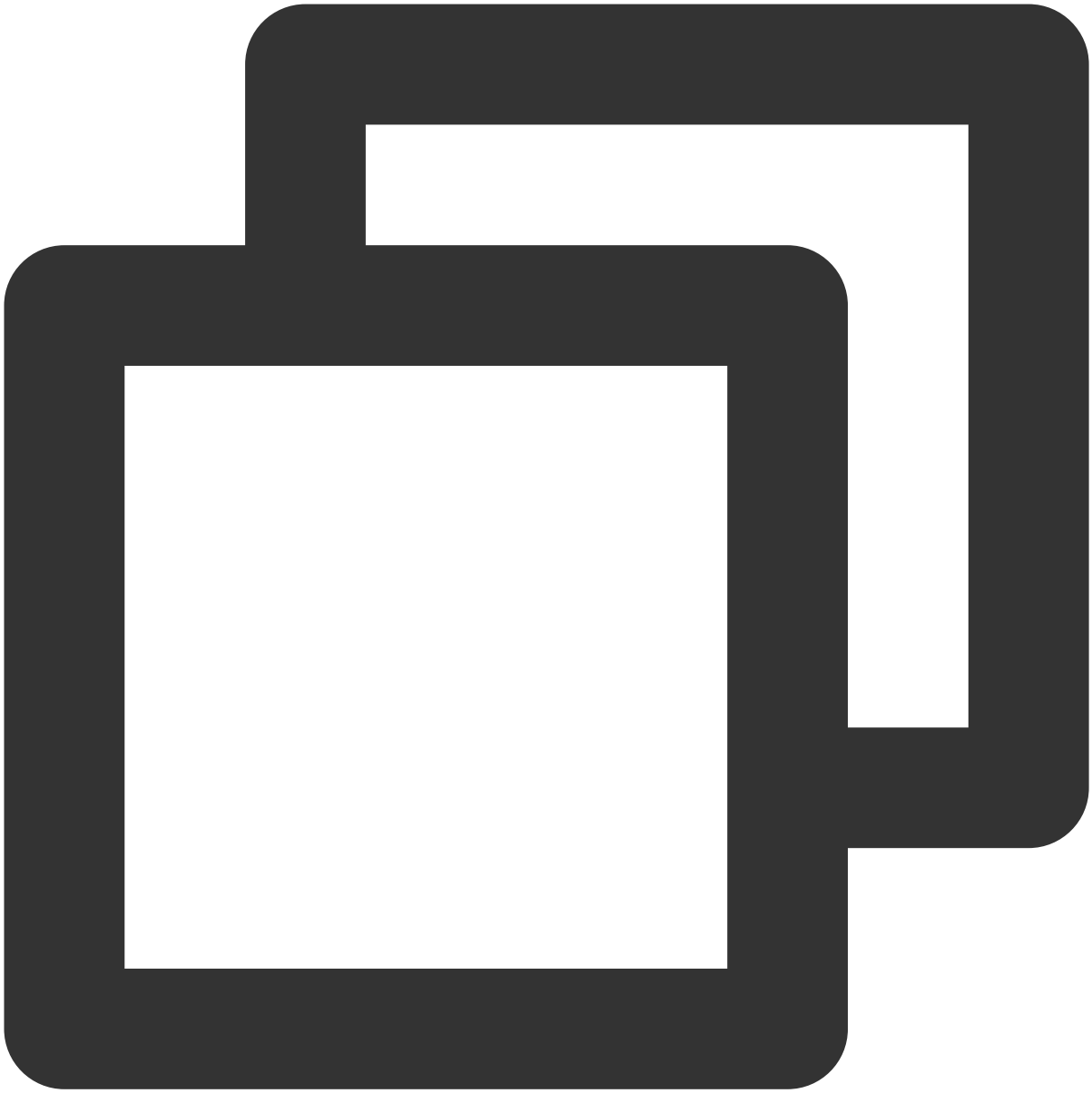
API 名称	API 描述	说明
AsymmetricSm2Decrypt	SM2 解密	请参见 AsymmetricSm2Decrypt
AsymmetricRsaDecrypt	RSA 解密	请参见 AsymmetricRsaDecrypt

本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

非对称解密

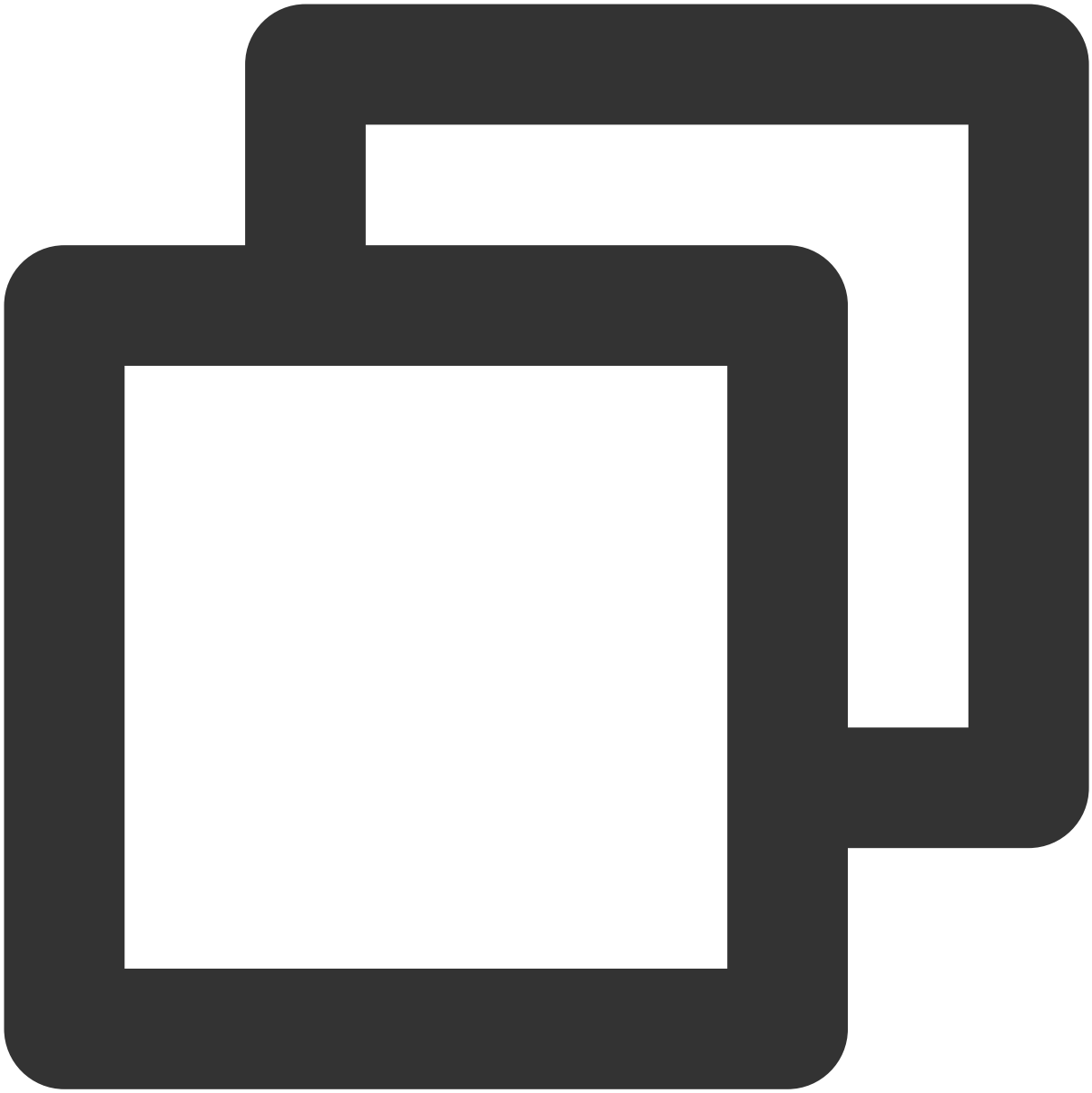
RSA 解密

输入



```
tccli kms AsymmetricRsaDecrypt --KeyId 22d79428-61d9-11ea-a3c8-525400****** --Algor
```

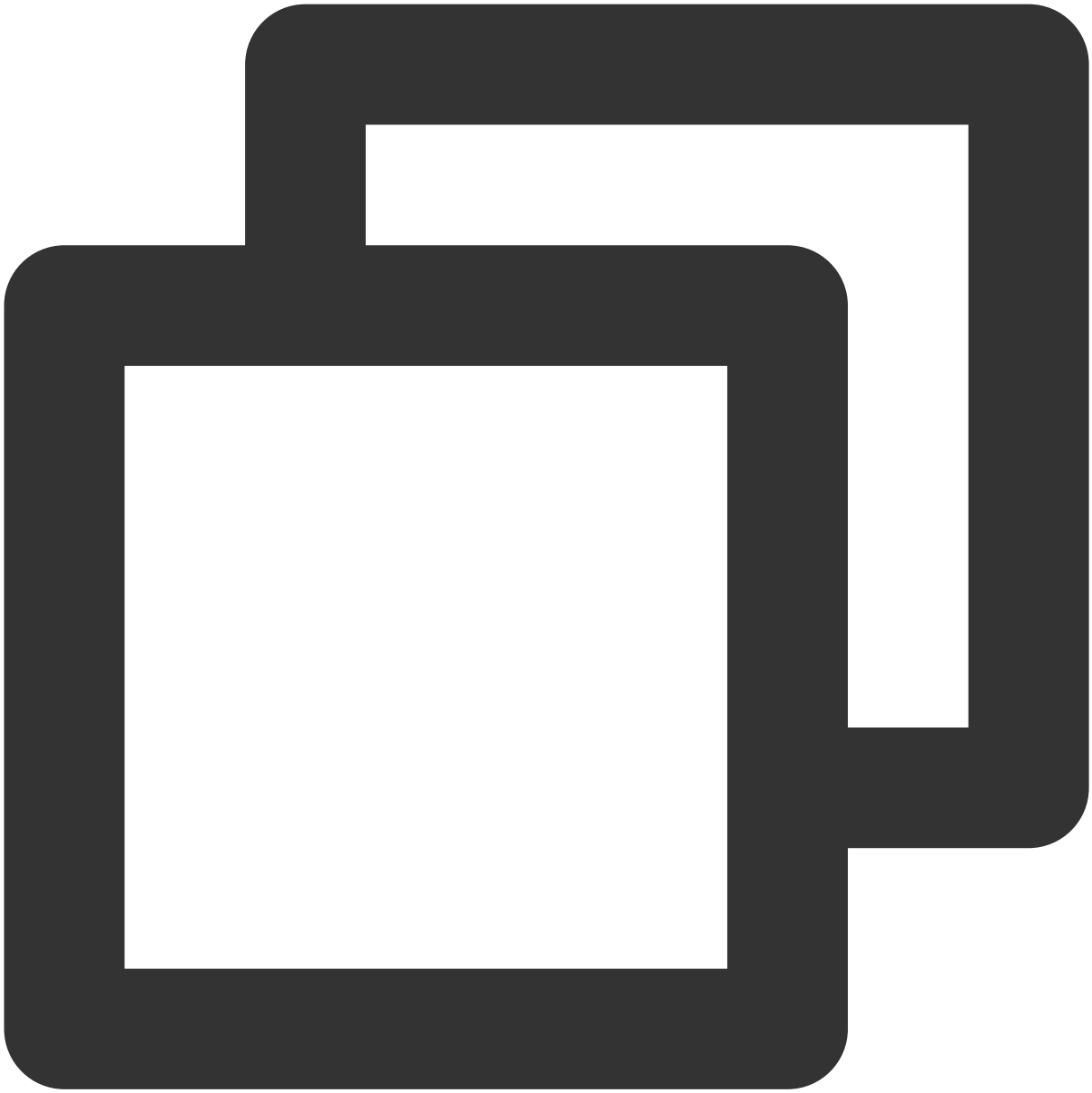
输出



```
{
    "Response": {
        "RequestId": "6758cbf5-5e21-4c37-a2cf-8d47f5******",
        "KeyId": "22d79428-61d9-11ea-a3c8-525400******",
        "Plaintext": "dGVzdAo="
    }
}
```

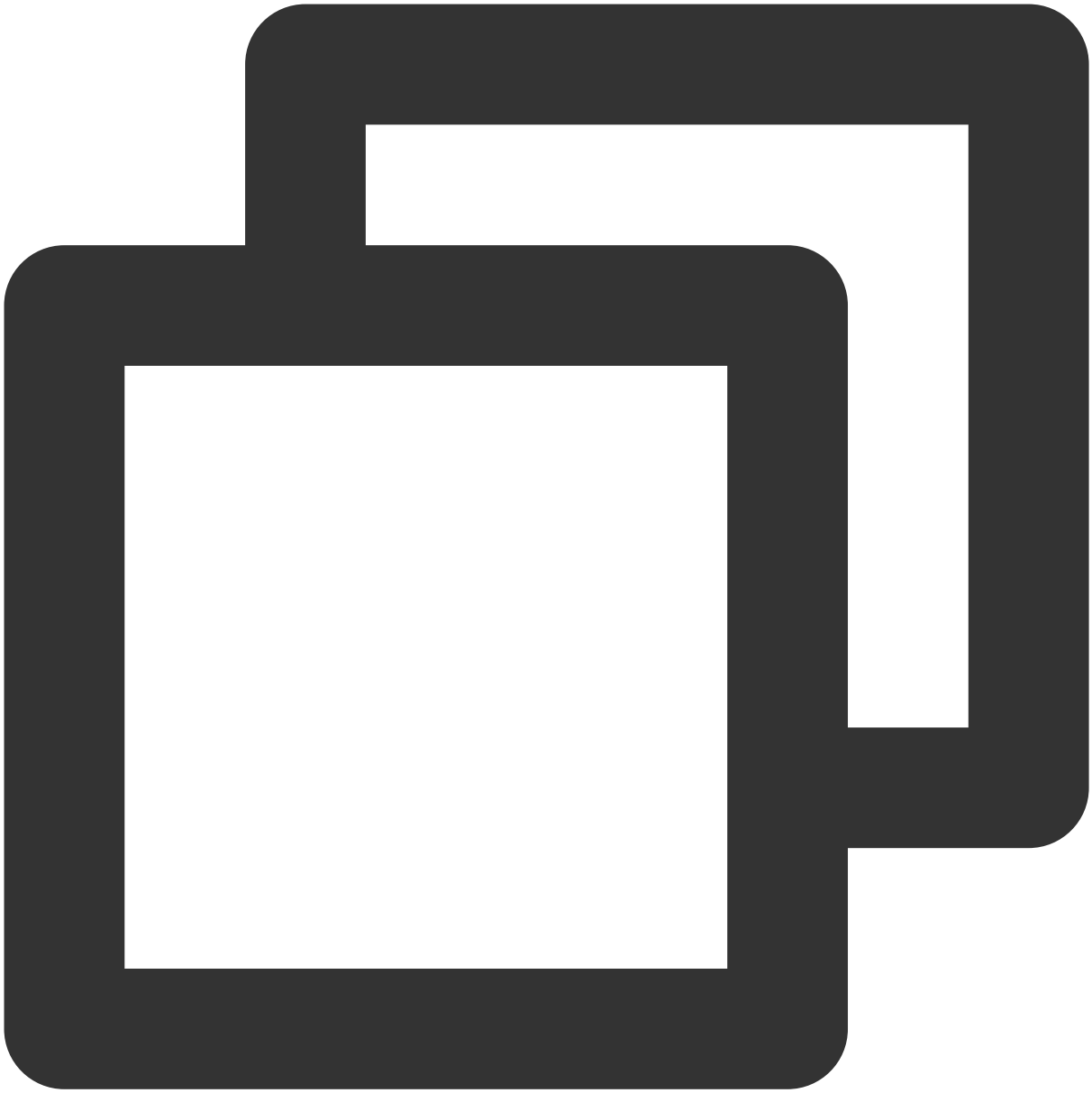
SM2 解密

输入



```
tccli kms AsymmetricSm2Decrypt --KeyId 22d79428-61d9-11ea-a3c8-525400****** --Ciphe
```

输出



```
{
    "Response": {
        "RequestId": "6758cbf5-5e21-4c37-a2cf-8d47f5******",
        "KeyId": "22d79428-61d9-11ea-a3c8-525400******",
        "Plaintext": "dGVzdAo="
    }
}
```

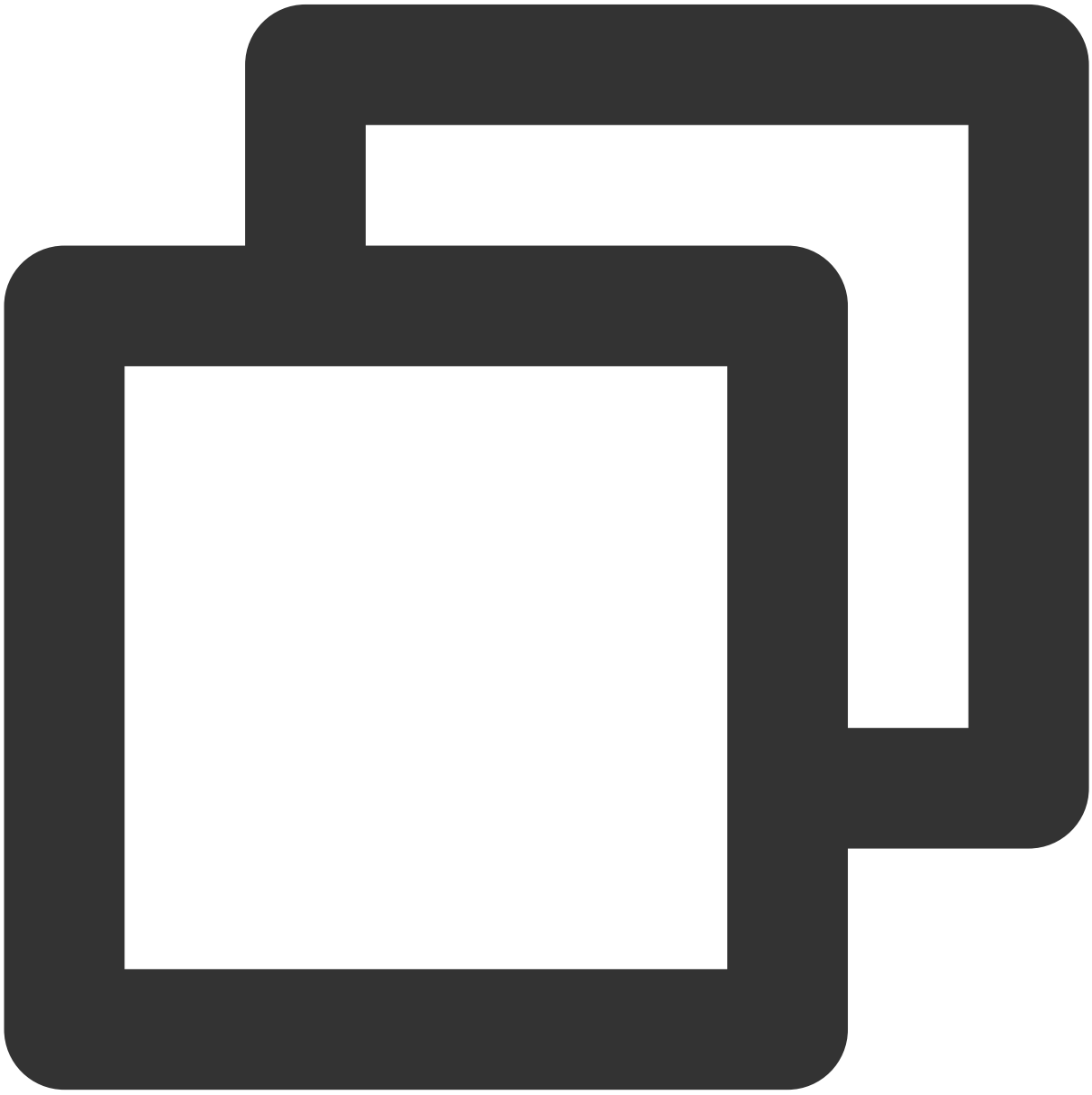
查看公钥

概述

获取指定 KeyId 的公钥信息，API 文档请参见 GetPublicKey。
本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

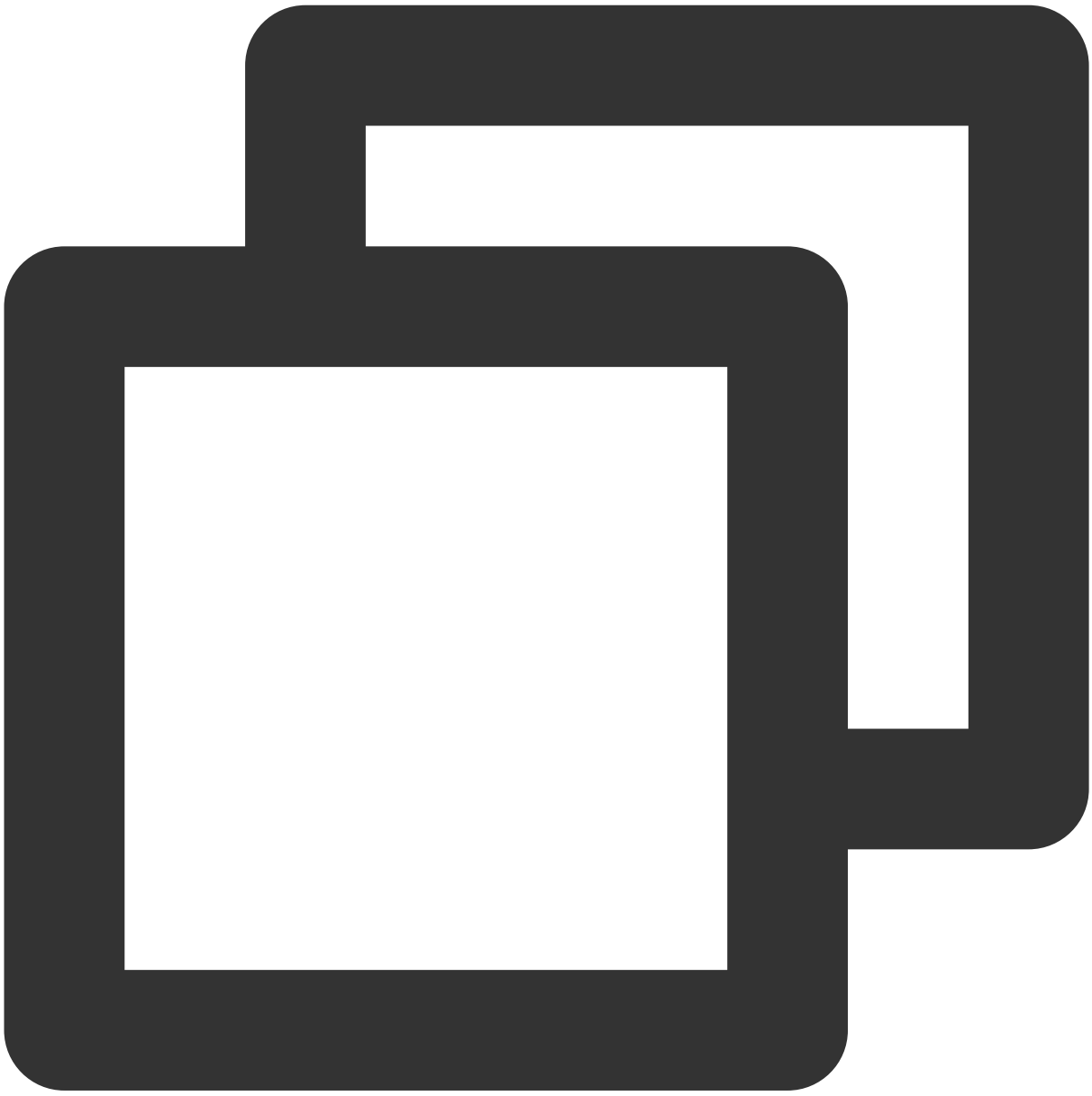
示例

输入



```
tccli kms GetPublicKey  --KeyId 22d79428-61d9-11ea-a3c8-525400******
```

输出：



```
{
    "Response": {
        "RequestId": "408fa858-cd6d-4011-b8a0-653805******",
        "KeyId": "22d79428-61d9-11ea-a3c8-525400******",
        "PublicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzQk7x7ladgVFEEGYD
        "PublicKeyPem": "-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCA
```

```
        }
    }
```

删除密钥

最近更新时间：2024-01-11 16:28:53

概述

计划删除密钥功能由两个 API 组成，相关分布如下：

API 名称	API 描述	说明
ScheduleKeyDeletion	添加计划删除任务	该 API 操作的 KeyId 和 PendingWindowInDays 为必选参数。
CancelKeyDeletion	取消计划删除任务	该 API 操作的 KeyId 为必选参数。

说明：

在密钥禁用的状态下通过 ScheduleKeyDeletion 接口设置 CMK 计划删除时间，在到了规定时间后，该密钥将自动被清理。

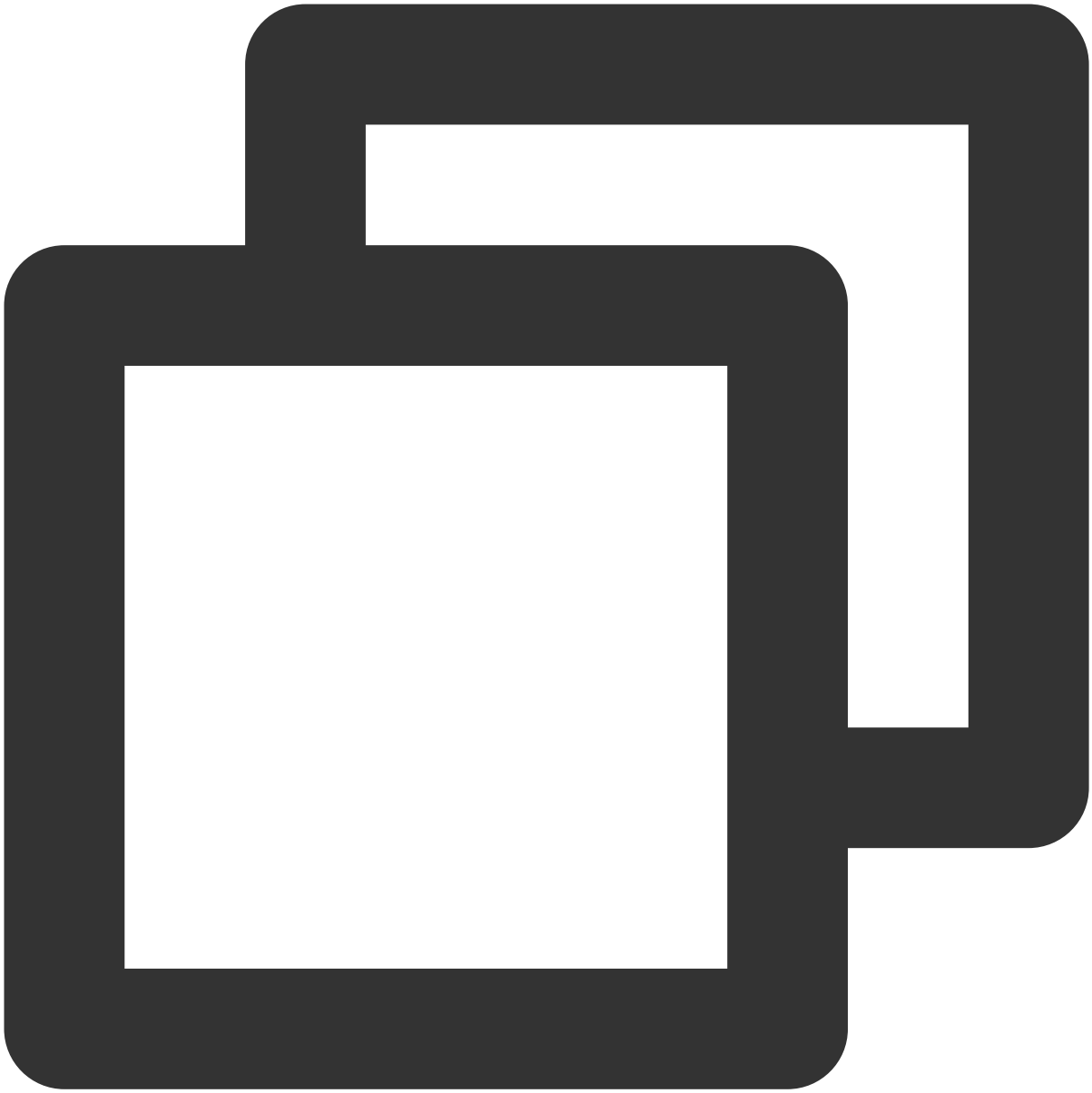
本文示例使用腾讯云 命令行工具 TCCLI，后续您可以使用任何受支持的编程语言调用。

示例

计划删除任务示例

现在我们对已经被禁用的指定 CMK 进行删除操作，计划7天后删除。

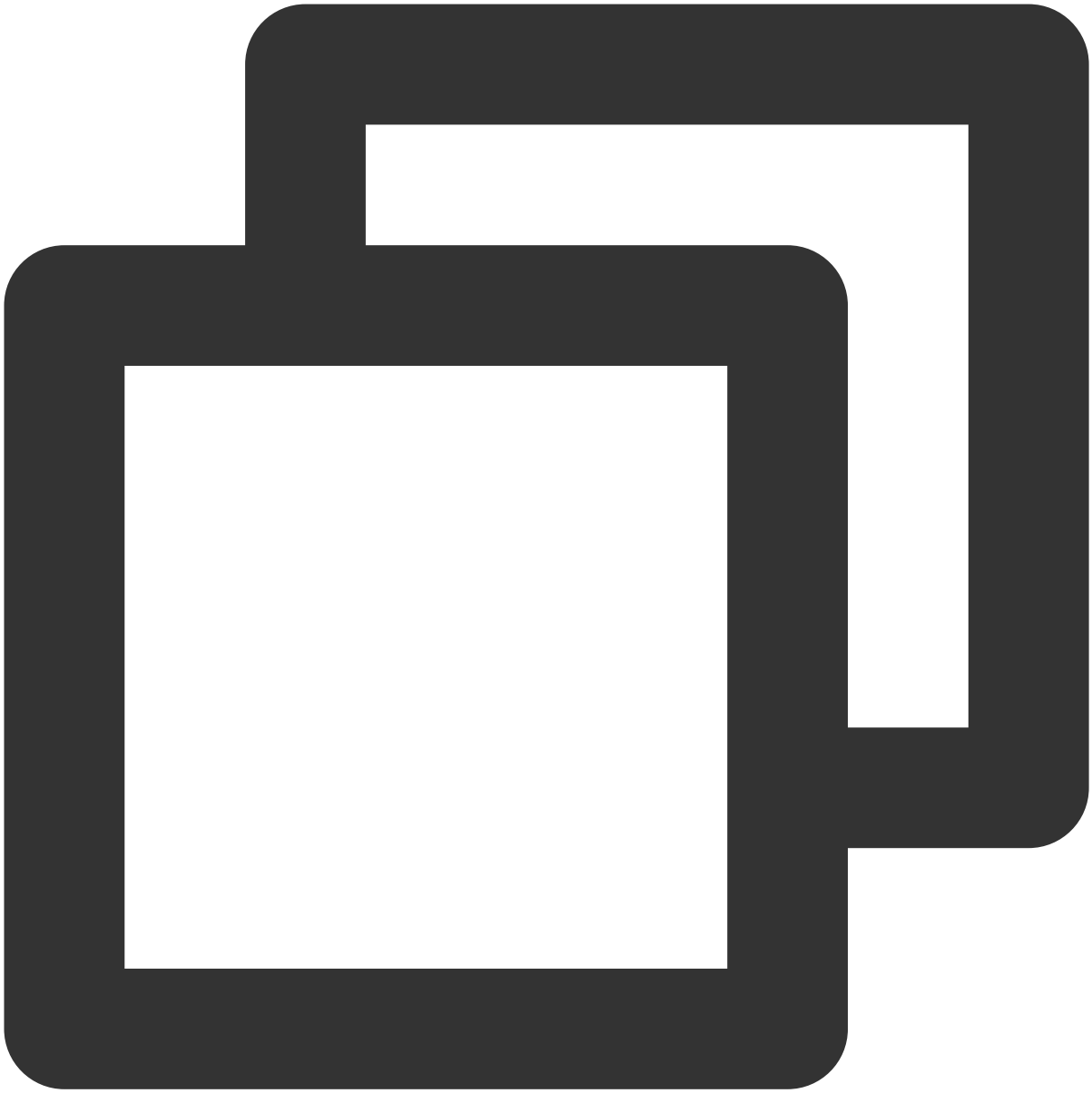
输入



```
tccli kms ScheduleKeyDeletion --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-5
```

输出

如果设置成功，返回请求将返回计划删除 ID 和计划删除时间戳。

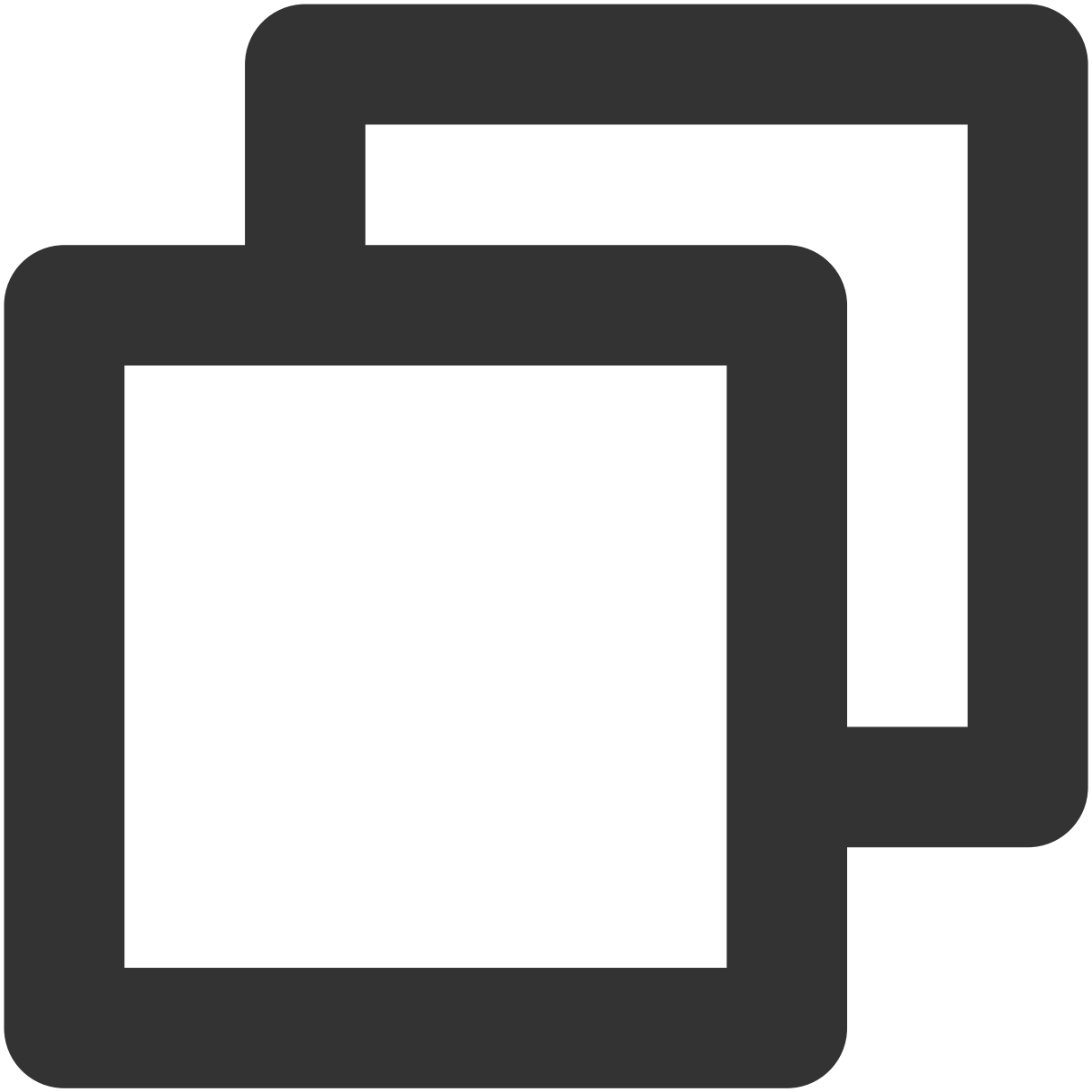


```
{
    "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09",
    "RequestId": "2bd72d85-f9dd-4465-ae51-beebff54f540",
    "DeletionDate": 1572512542
}
```

取消删除计划任务示例

现在我们来取消指定 CMK 的删除计划任务，其中示例流程中的 CMK 以上述创建的 CMK 为例。

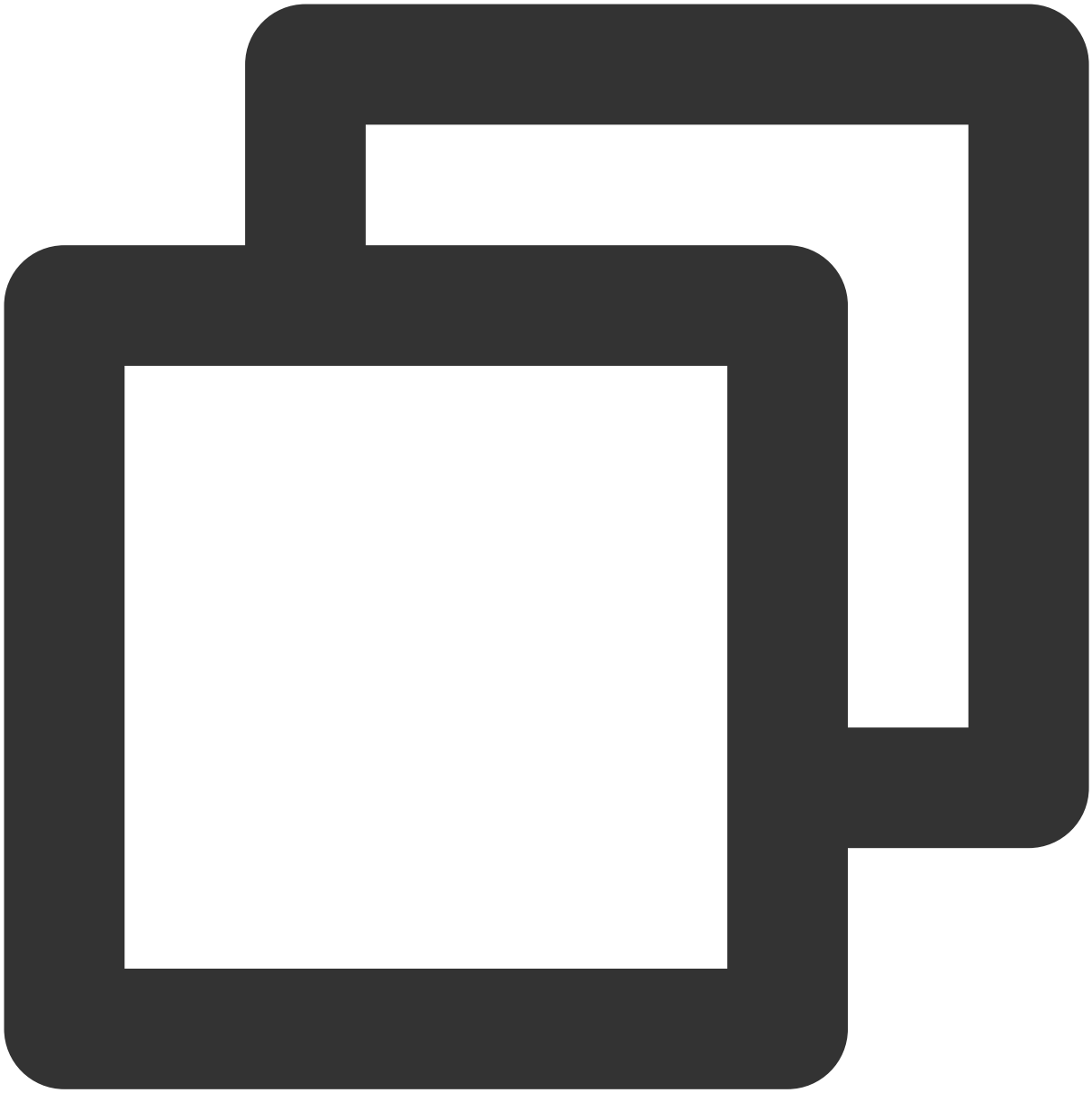
输入



```
tccli kms CancelKeyDeletion --region ap-guangzhou --KeyId 5xxxxx-xxxx-xxxx-xxxx-52x
```

输出

如果执行成功，返回请求中将包含被成功取消删除计划的 CMK ID。



```
{
    "KeyId": "6xxxxxxx-xxxx-xxxx-xxxx-5xxxxxxxxc09",
    "RequestId": "c85473c6-e18d-4a09-9eac-03958dd4714d"
}
```