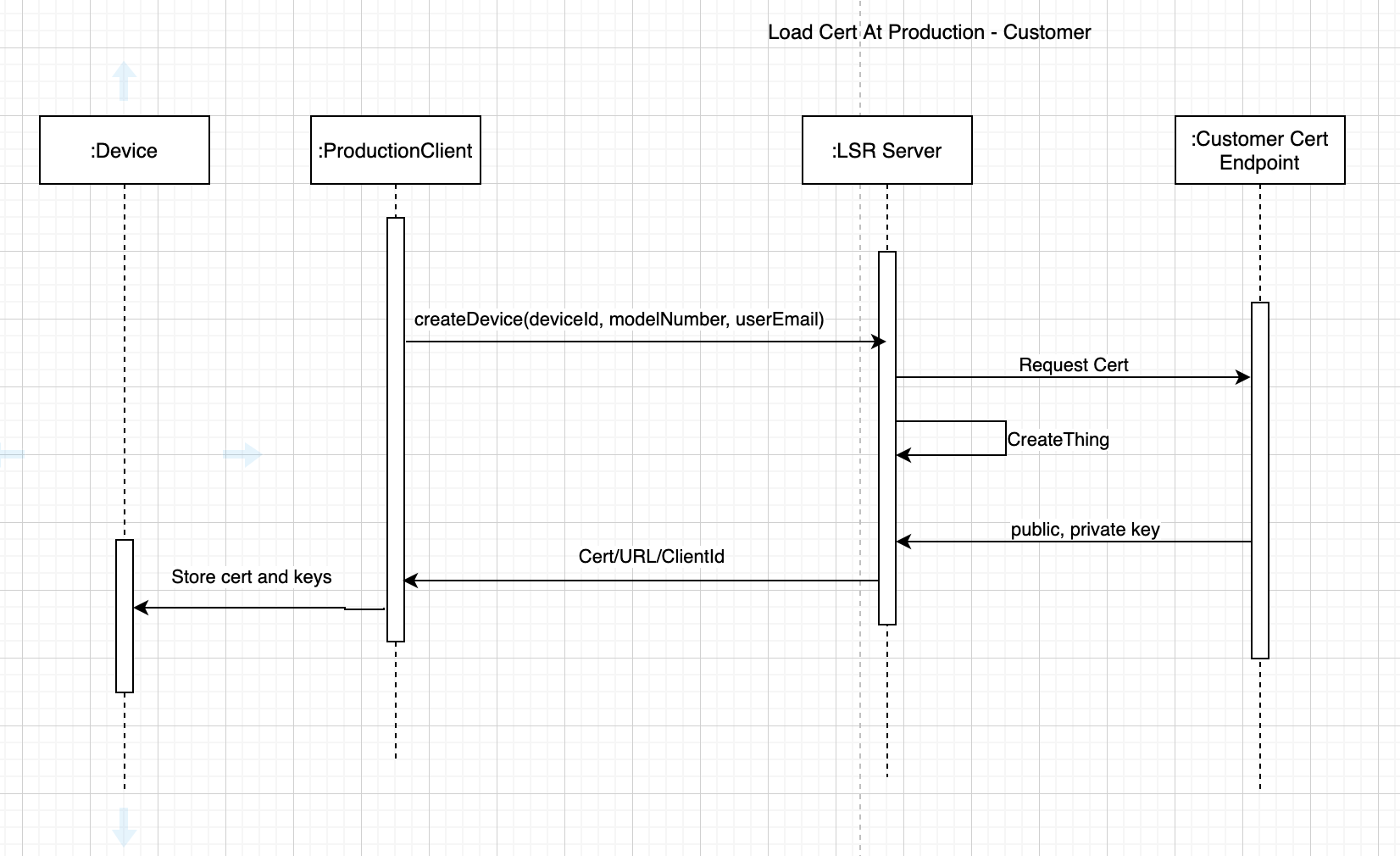
# 证书请求

此API由客户实现, MioConnect发起请求获得证书, 并加载到设备内. 此API适用于客户希望设备使用自己CA签发的证书, 达到客户内部安全标准.

## 时序图



## Authentication

MioConnect使用如下方式和客户服务器验证身份.

### Mutual TLS

操作步骤:

1. 用户在MioConnect控制台登录
2. 进入设备证书管理页面
3. 证书获取选项选择使用自己的证书
4. 输入证书服务器地址
5. 验证方式选择Mutual TLS, 上传MioConnect请求连接时需要的client certificate, 包括私钥, 公钥.
6. 点击保存按钮.

## API

### Request Device Cert

POST /devicecert

**Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | In | Description |
| deviceId | string | body | 设备序列号 |
| modelNumber | string | body | 设备模型 |

**Response**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | In | Description |
| certificateId | string | body | id for generated certificate |
| certificatePem | string | body | client certificate for device, in pem format |
| keyPair.publicKey | string | body | public key for client keypair |
| keyPair.privateKey | string | body | private key for client keypair |
| rootCertPem | string | body | root certificate from 3rd-party CA, in pem format |
| createdAt | string | body | created time for client certificate,Unix timestamps in seconds. For example, 1621316605 is Tuesday May 18 2021 5:43:25 GMT |

Status: 201 Created

{

“certificateId“: ,

"certificatePem": ,

"keyPair":

{

"publicKey":

"privateKey":

},

“rootCertPem":

"createdAt":

}

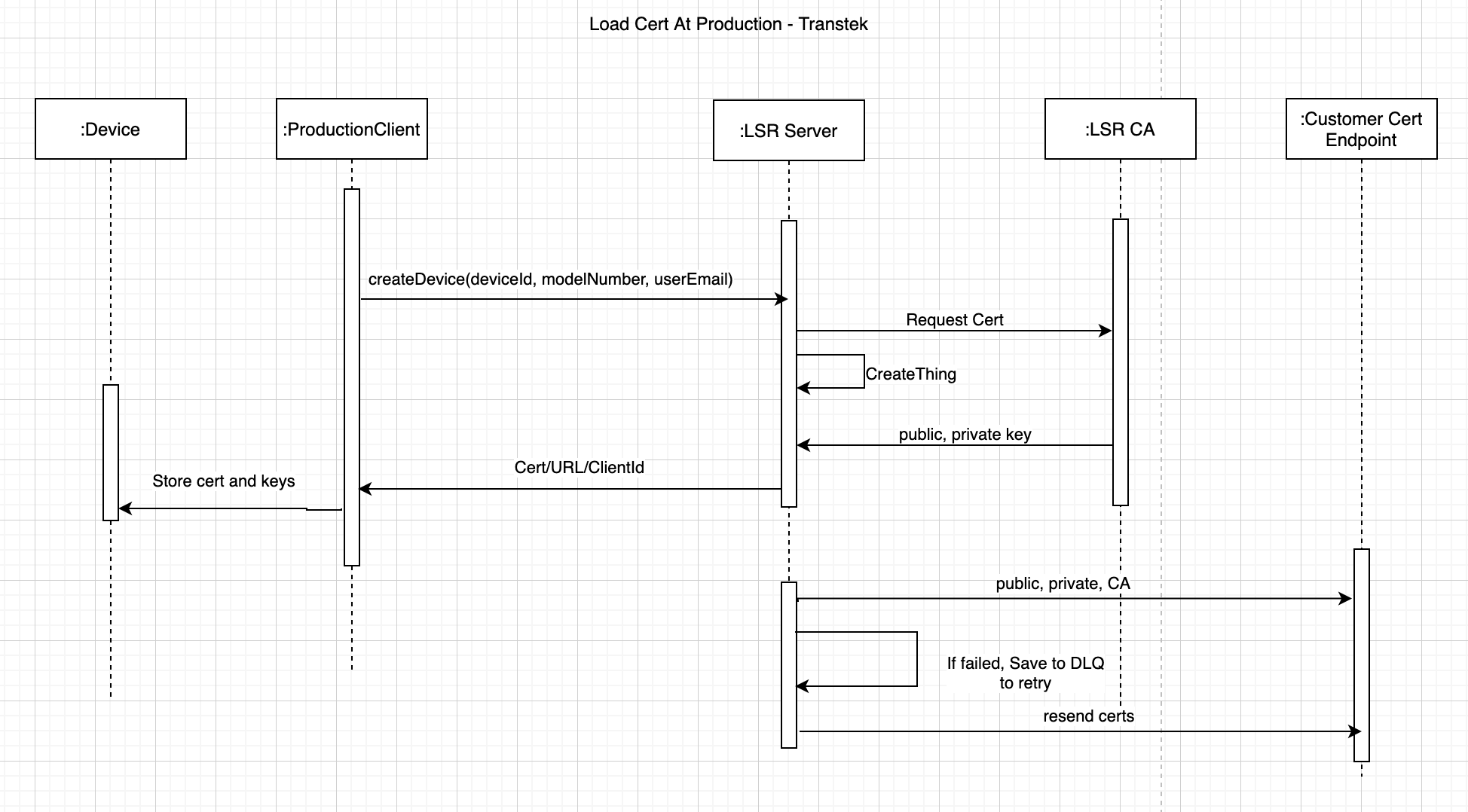
**Forbidden**

Status: 403 Forbidden

# 证书同步

此API由客户实现, MioConnect通过自己的CA获得证书并成功加载到设备后, 发起请求, 将生成的证书同步给客户服务器. 客户服务器可以使用此证书校验设备身份. 此API适用于客户希望使用MioConnect签发证书, 并在自己服务器端验证请求连接的设备身份.

时序图



## Authentication

MioConnect使用如下方式和客户服务器验证身份.

### Mutual TLS

操作步骤:

1. 用户在MioConnect控制台登录
2. 进入设备证书管理页面
3. 证书获取选项选择使用MioConnect证书
4. 输入同步证书服务器地址
5. 验证方式选择Mutual TLS, 上传MioConnect请求连接时需要的client certificate, 包括私钥, 公钥.
6. 点击保存按钮.

## API

### Sync Device Cert

POST /syncdevicecert

**Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | In | Description |
| deviceId | string | body | 设备序列号 |
| modelNumber | string | body | 设备模型 |
| certificateId | string | body | id for generated certificate |
| certificatePem | string | body | client certificate for device, in pem format |
| keyPair.publicKey | string | body | public key for client keypair |
| keyPair.privateKey | string | body | private key for client keypair |
| rootCertPem | string | body | root certificate from 3rd-party CA, in pem format |
| createdAt | integer | body | created time for client certificate,Unix timestamps in seconds. For example, 1621316605 is Tuesday May 18 2021 5:43:25 GMT |

**Response**

Status: 200 OK

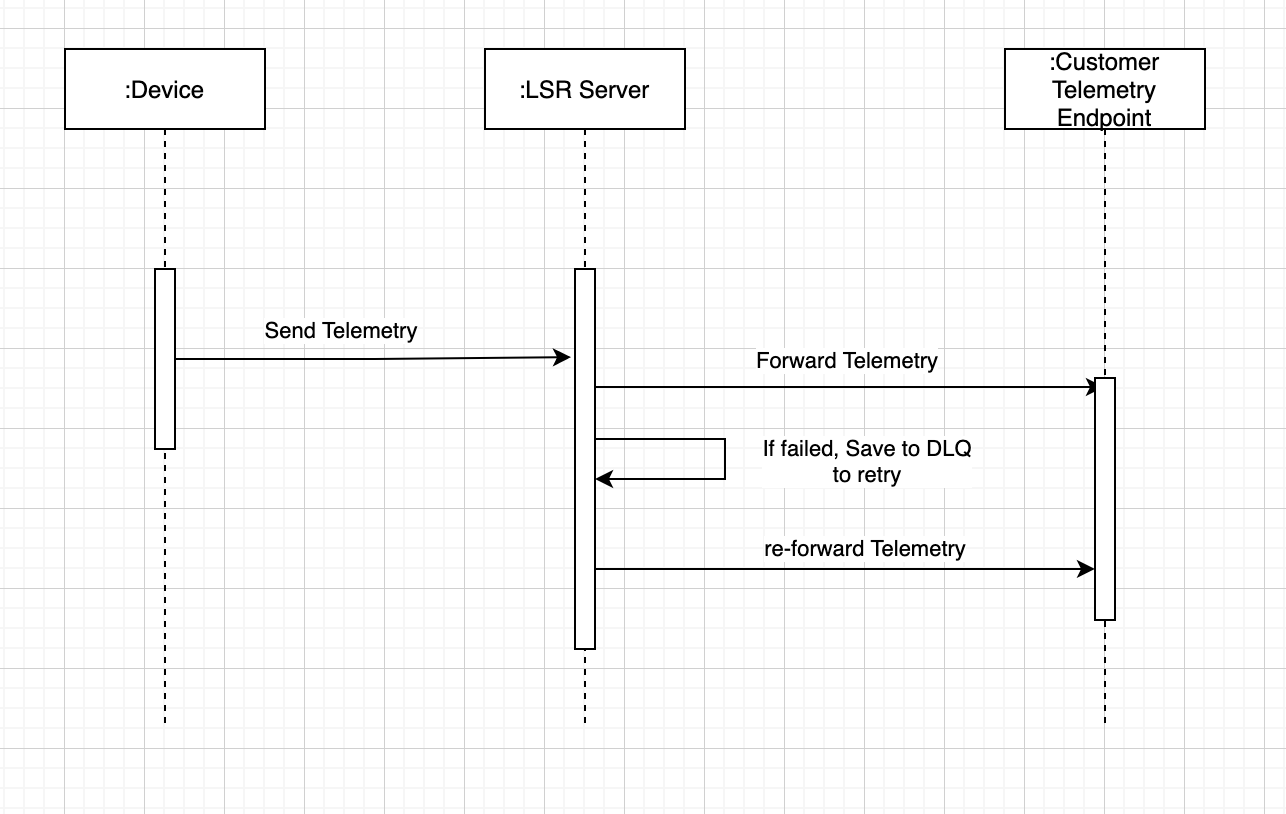
**Forbidden**

Status: 403 Forbidden

# Telemetry Forwarding

Telemetry Forwarding(TF) defines the API to receive telemetry data forwarded from MioConnect cloud. You will need to implement TF API on your end, based on the specification below. When your device sends data to MioConnect Cloud, MioConnect Cloud will forward it to your endpoint.

时序图



## Authentication

MioConnect使用如下方式和客户服务器验证身份.

### Mutual TLS

操作步骤:

1. 用户在MioConnect控制台登录
2. 进入设备证书管理页面
3. 证书获取选项选择使用MioConnect证书
4. 输入同步证书服务器地址
5. 验证方式选择Mutual TLS, 上传MioConnect请求连接时需要的client certificate, 包括私钥, 公钥.
6. 点击保存按钮.

## API

### Forward Telemetry

POST /forwardtelemetry

**Parameters**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | In | Description |
| deviceId | string | body | 设备序列号 |
| createdAt | integer | body | time for the record to be created on MioConnect server. It could be different than created time from device side, since device may not be able to send data in time. |
| data | json | body | data includes original data from device, in json format. |

**Response**

Status: 200 OK

**Forbidden**

Status: 403 Forbidden