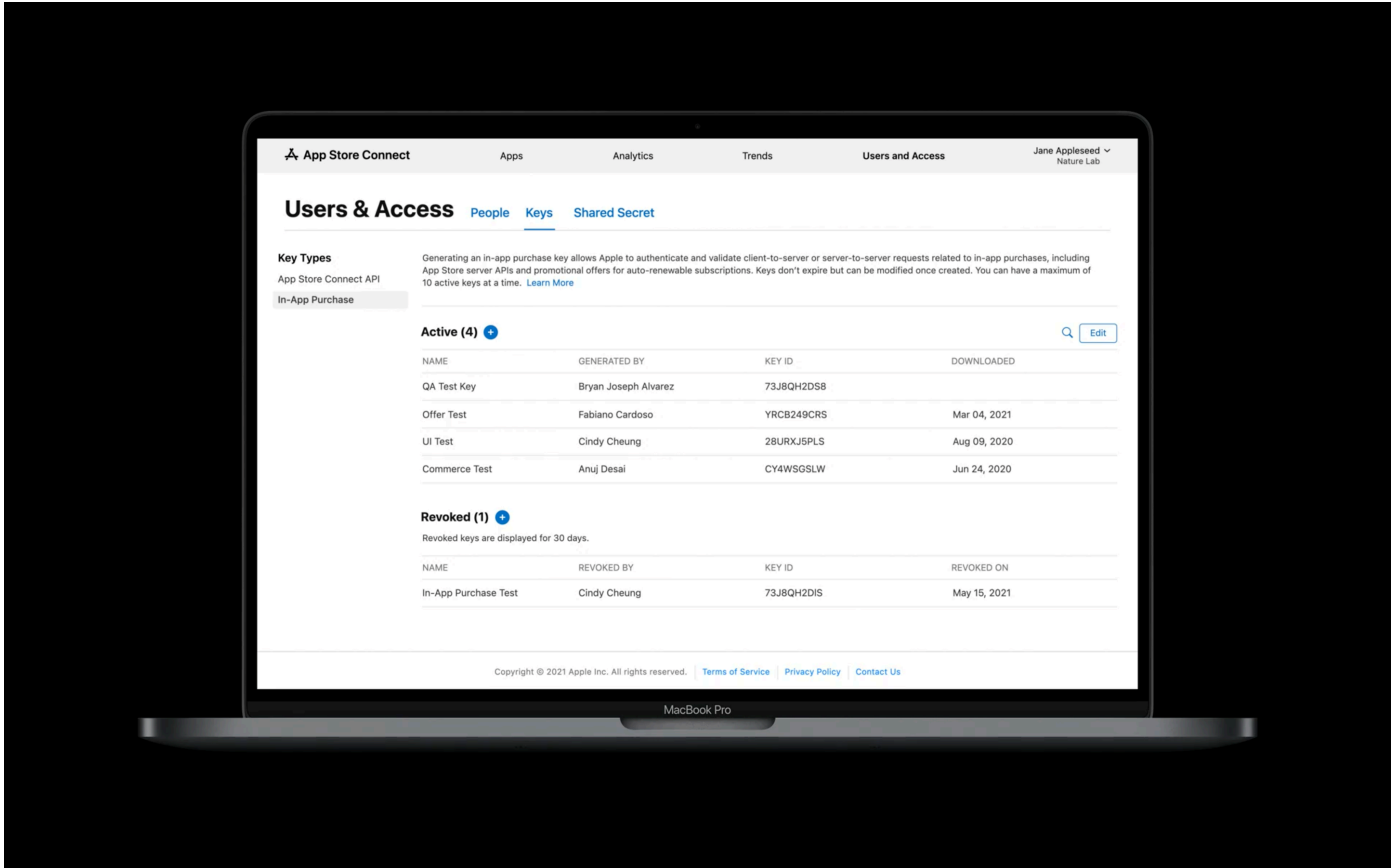


# JWT —— 用于保障后台接口安全调用

注意，上述提到的 Subscription Status API & In-App Purchase History API 均采用 JWT 验证，我们需要执行以下步骤

1、从 App Store Connect 配置 **In-App Purchase Keys**（参考下图）（没错，又是一个新的 Key，截止目前，已有共享密钥、App 专用共享密钥、促销优惠密钥、In-App Purchase Keys 等四类 IAP 相关的密钥）



4.png

- 2、从 App Store Connect 中获取 KeyID，用于放置 JWT header.kid 字段
- 3、从 App Store Connect 中获取 IssuerID，用于放置 JWT payload.iss 字段
- 4、使用 ES256 算法及 In-App Purchase Keys 私钥对请求进行签名
- 5、将头部、内容部分及签名部分通过逗号拼接，获得 JWT，用于请求相关 API

```
// JWT token
```

```
Base64(header) + "." + Base64(payload) + "." + sign(Base64(header) + "." + Base64(payload))
```

```
// header
```

```
{  
  "kid": "CYWSGSLW",  
  "alg": "ES256",  
  "typ": "JWT"  
}
```

```
// payload
```

```
{  
  "iss": "2ce111ac-b5be-11eb-8529-0242ac130003",  
  "iat": 1623081000,  
  "exp": 1623083000,  
  "aud": "appstoreconnect-v1",  
  "nonce": "nonce123",  
  "bid": "co.oceanjournal"  
}
```

5.png

注意：签发时间 iat 与过期时间 exp 相隔必须在一小时内