标准包 Ukey 变更业务文档

吴鼎

2024 年 2 月 19 日

需求概述：

- 需求编号: PRIV-4388
- 影响项目: 标准包前台 (PC，H5)，标准包后台
- 上线版本: 4.3.8
- 上线时间: 2024-01-11
- 相关人员
  - 产品: 周琪
  - 前端: 吴鼎 (PC)，李潇宇 (H5)，王可
  - 后端: 李新田，徐家豪，袁帅 (Q 上海)，詹善明
  - 测试: 刘静 (Q 上海)，苗含玉

修改记录：

时间	需求号	版本	修改人	更新内容
2024-02-05	PRIV-4388	4.3.8	吴鼎	需求上线，首次编写业务文档

目录

1 功能概述

标准包前/后台新增 Ukey 变更订单类型，支持用户变更当前 Ukey 内的证书，使用场景包括:

- 单位名称发生变更后，客户希望将原 ukey 进行变更，不浪费硬件设备
- 证书不满足要求，需要重新烧制
- 个人证书需要更换成单位证书

整体流程如图1.1:

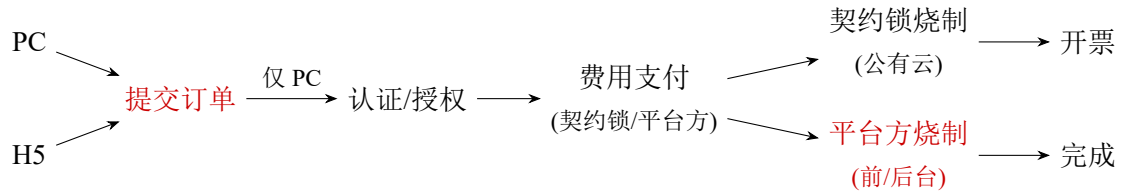


图 1.1 Ukey 变更整体流程

上述几个步骤的功能简要概述为:

- 后台配置: 进入标准包后台: 数字证书/Ukey 变更进行参数配置，如果前台登陆的账号不满足配置条件则不显示 Ukey 变更入口。
- 提交订单: 用户进入 Ukey 变更界面后选择需要变更的 Ukey(PC 可以选中插入的 Ukey)，填写新证书信息以及章面信息、，然后提交订单
- 认证授权: 该步骤可跳过。
  - 如果申请主体未认证，则需完成认证流程
  - 如果替他人申请证书，则需申请主体登录后授权
- 费用支付: 在后台可配置两种费用支付方式:
  - 支付给契约锁: 走公有云烧制流程
  - 支付给平台方: 走私有云烧制流程，在私有云前后台均可烧制
- 烧制: 本次开发为平台方烧制，前后台均可走烧制流程，先申请证书，然后 (在插入 Ukey 情况下) 将证书写入 Ukey
- 开票: 仅在契约锁烧制的 Ukey 可开票

其中红色部分: 提交订单，平台方烧制为本次主要开发流程。

2 提交订单

提交订单的逻辑整体上复用 Ukey 新购逻辑。

2.1 后台配置

申请主体　控制可进行 Ukey 变更的主体，包括内外部单位，内外部个人。如果前台登陆的用户不满足主体筛选条件，则不展示 Ukey 变更入口。前台 Ukey 变更入口 (侧边栏菜单) 由后台接口控制。

通道选择　标准包仅支持契约锁通道，该配置项主要用于项目定制化需求。

支付方式　Ukey 变更配置项相比 Ukey 新购少一个烧制方式，配置完支付方式后自动选择对应的烧制方式。主要支付方式的影响如表1:

表 1　支付方式配置项

支付方式	含义	烧制方式
支付给平台方	私有化费用分摊，走私有云烧制流程	平台方烧制/用户自主烧制
支付给契约锁	契约锁收费，走公有云烧制流程	契约锁客服烧制

此外，还可能出现**不支付**选项，这代表私有云系统启用了费用分摊功能，但没有配置相关的规则，此时仍然走私有云烧制流程。

可用证书　可用证书包括可用 RSA 证书与可用 SM2 证书，该配置项会出现三种情形:

- 无可用 RSA/SM2 证书: 自建通道禁止某一项，则只给我文本提示: 当前自建通道无法申请当前算法长期证书
- 有特定的 RSA/SM2 证书范围: 通过多选组件选择可用的 CA 机构
- 能开启 RSA/SM2 证书: 通过开关控制能否启用 RSA/SM2 证书

可选年限　可选年限包括一年期与两年期，可以选择一个或所有。如果都不选，那么前台不会展示 Ukey 变更入口。

是否需要烧制章面　该配置项有三个单选项: 需要章面，无需章面，由用户自主选择。前两个选项会强制用户制作/不制作章面。

上述的所有配置会在用户提交订单时生成一份快照，即以用户提交时的配置为准。如果后续更改了配置，不影响先前已提交的订单。

2.2 Ukey 变更入口

Ukey 变更前台界面的路由为: `/cert-apply?orderType=UKEY_CHANGE`。所有 Ukey 变更入口都通过改变路由进入变更界面。目前主要有以下几类入口:

- 常规申请: 前台证书界面，点击证书服务的 Ukey 变更按钮
- 跳转申请: 首页，个人中心，合同签署等界面跳转至 Ukey 变更界面
- 开放平台: 开放平台生成路由链接跳转至 Ukey 变更界面

常规申请是最常见的 Ukey 变更订单申请方式，进入变更界面后，系统将获取后台配置并提供各字段的选项。

跳转申请会根据来源不同对部分字段作限制，需要限制的字段会出现在路由上，例如通过 `userCenterSigAlgType` 选中默认算法，通过 `renew` 知道来自个人中心，需要进行相关的初始化操作。

开放平台申请的链接在路由上会有 `viewToken` 字段，进入界面后，系统会根据 `viewToken` 查询相关配置，并对订单信息做一定限制。

三类入口填写证书信息获取配置与进行限制的逻辑如图2.1:

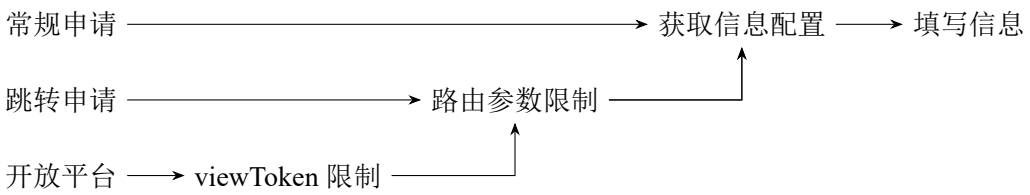


图 2.1 提交订单入口配置逻辑

2.3 Ukey 信息填写

2.3.1 指定需要变更的 Ukey

目前支持两种指定 Ukey 的方式：选择 Ukey 与插入 Ukey。H5 仅支持选择 Ukey。

选择 Ukey 系统将返回**当前私有化系统**中用户身份所管理的**订单的 Ukey** 列表，如果 Ukey 存在变更中的订单，则置灰不允许选中，否则可以选中。选中后点击详情可获得 Ukey 相关的信息。

插入 Ukey 用户插入一个契约锁颁发的 Ukey，系统将自动识别并获取其相关信息。在插入 Ukey 模式下，即使是**非当前私有化系统**的 Ukey 也可进行变更。非当前私有化系统的 Ukey 无法通过接口获取完整的信息，因此 Ukey 信息会出现显示不全的情形。

2.3.2 其他信息填写

其他信息与 Ukey 新购基本一致，Ukey 变更包含两部分信息: 新证书信息与章面信息 (如果禁止制章则不存在章面信息)。

用户在选择单位/个人时，列表会给出认证状态，如果主体未认证，则需完成认证流程。如果选中的主体与当前使用的身份不符，则会通知对方授权，授权后继续支付流程。

用户在填写完基本信息后，界面右上角会显示 Ukey 变更的价格，点击提交订单即可。

如果变更的 Ukey 在当前私有化系统中存在章面信息，提交订单后会给出相关提示。

详细逻辑图

提交 Ukey 变更订单的详细逻辑如图2.2所示:

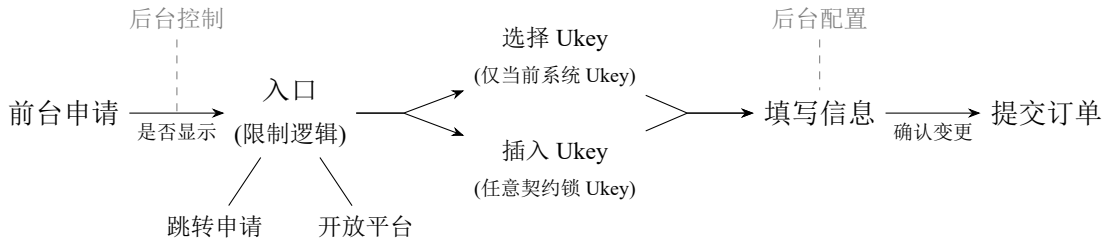


图 2.2 提交订单详细逻辑

3 平台方烧制

私有化开启费用分摊功能，Ukey 变更选择平台方支付，在付费后进入烧制流程。此时前台和后台均可烧制 Ukey。

烧制过程是部分可中断的，如果弹窗/提示框存在取消或关闭按钮，用户可自行中断当前步骤，但如果不存在关闭按钮，请不要中断正在执行中的任务，不要关闭浏览器页面或操作系统，否则可能产生不必要的麻烦。

3.1 证书申请

走到烧制流程后，进入订单详情界面，会显示待烧入 Ukey 的证书基本信息以及**申请证书**按钮。点击按钮会依次检测驱动状态，检查 Ukey 是否为变更订单中指定的 Ukey。如果均满足条件则显示烧制弹窗，等待用户确认信息，并填写新 Ukey Pin 码。

3.1.1 清空 Ukey

确认新 Pin 码后，系统给出*正在向 CA 机构申请证书*弹窗，并清空插入的 Ukey，前端首先调用驱动的以下两个方法:

```
ukeySocket.clearUkey();
ukeySocket.changePin({ NewPIN: pin, OldPIN: '12345678' });
```

这两个方法分别清空 Ukey，设置新的 Pin 码。在驱动的两个方法调用结束后，再次调用后端的 Ukey 初始化方法:

```
// 接口路径: /cert/order/ukey/init
Apis.CertApply.ukeyInit(orderDetail.certOrder.id, ukeySocket.deviceId);
```

此时 Ukey 完成初始化操作。注意，在此过程中弹窗并不会给出关闭按钮，因此不允许中断清空 Ukey 过程，如果此时过程被中断，可能会出现 Ukey 已被初始化，但后端没有记录等问题。

3.1.2 申请证书

清空 Ukey 后，系统自动进入申请证书流程，此时弹出*正在向 CA 机构申请证书*弹窗，同时根据所申请的证书算法类型不同，分别调用驱动的获取 P10 方法:

```
// RSA 算法，对应 C++ 方法: requestRSAP10
ukeySocket.getRSAP10({ name: certDetail.tenantName, docId: certDetail.docId })
// SM2 算法，对应 C++ 方法: requestP10
ukeySocket.getSM2P10({ name: certDetail.tenantName, organizationUnit: certDetail.docId })
```

获取 P10 信息后，调用后端的申请证书方法:

```
// 接口路径: /cert/order/ukey/applycert
```

```
Apis.CertApply.ukeyApplyCert({
    orderId: orderDetail.certOrder.id,
    p10,
    ukeyCntName,
    ukeyNum: ukeySocket.deviceId,
}).silence().then(() => applyCallback());
```

该接口会向 CA 机构申请证书，因此响应较慢。

申请证书过程可以中断，关闭弹窗后，后端仍然处于申请证书的过程中，此时退出界面没有影响。如果已申请完成，再次进入会显示烧制界面。

3.2 证书写入

证书申请完成后会自动进入写入流程，如果申请过程中退出了界面也可通过订单详情界面的写入证书按钮进入写入流程。

写入过程首先会调用后端的写入接口:

```
// 接口路径: /cert/order/ukey/write
Apis.CertApply.ukeyWriteCert(orderDetail.certOrder.id, ukeySocket.deviceId)
    .then((resultWrite) => {
    // 可以写进ukey了
    if (resultWrite.pubCert || resultWrite.doubleCertData) {
        MessageBox.close();
        Message.success('申请成功');
        // 开始写入驱动
        writeCertToUkey({ ukeySocket, resultWrite, pin, orderDetail, createElement, callback:
            writeCallback });
    }
})
.catch(() => {
    clearInterval(writeTime);
});
```

通过该接口获取下载的证书，并尝试写入驱动，此时界面给出 正在将证书写入 *UKey* 弹窗，同时调用驱动的写入证书方法:

根据证书算法类型与是否为双证调用如下任一方法将证书写入 Ukey:

```
// RSA 双证，对应 C++ 方法: importRSADoubleCertOnPrivate
ukeySocket.importRSADoubleCert(JSON.parse(resultWrite.doubleCertData))
// RSA 单证，对应 C++ 方法: importRSACert
ukeySocket.importRSACert({ data: resultWrite.pubCert, pin, ukeyCntName: '' })
// SM2 双证，对应 C++ 方法: importSM2DoubleCert
ukeySocket.importSM2DoubleCert(params)
// SM2 单证，对应 C++ 方法: importSM2Cert
ukeySocket.importSM2Cert({ data: resultWrite.pubCert, pin })
```

证书写入完成后，如果存在图片 (章面/签名)，再调用如下方法写入图片:

```
// 对应 C++ 方法: importSealWithName
ukeySocket.setUkeySealImg({ fileName: imgName, data: base64SealImg })
```

以上两个写入步骤均成功执行后，调用后端的成功写入证书方法:

```
// 接口路径: /cert/order/ukey/writesuccess
Apis.CertApply.ukeyWriteSuccess(orderDetail.certOrder.id);
```

此时写入过程结束，系统界面将刷新。

写入过程是不可以中断的，以上三个过程如果仅执行部分，会导致后端数据错误。如果任一过程失败，ukey 将被清空，回到写入前的状态。

部分 CA 机构 (辽宁 CA) 的下载证书接口是异步执行的，因此前端会轮询调用接口。

详细逻辑图

烧制 Ukey 的详细逻辑如图3.1所示 (红色为不可中断过程，蓝色可中断):

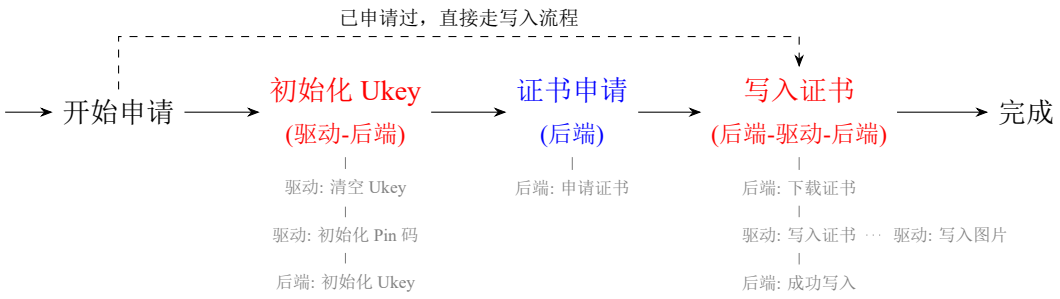
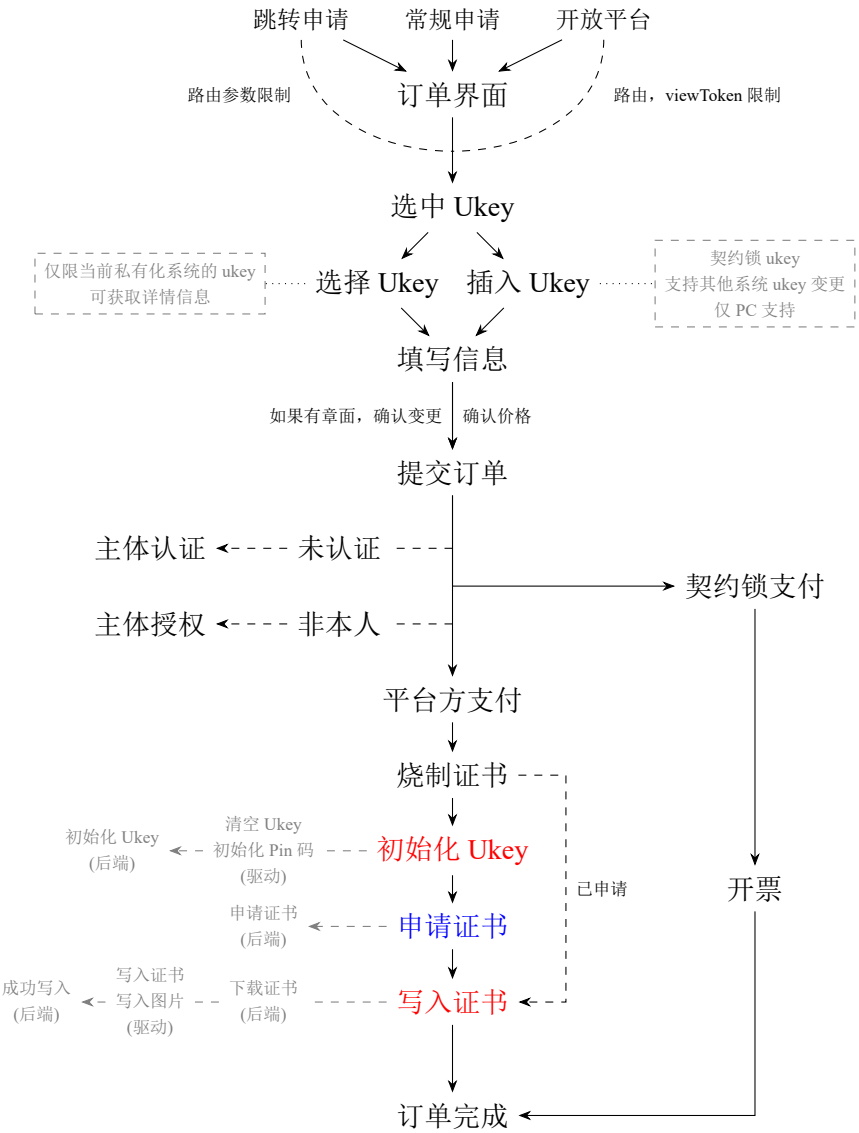


图 3.1 烧制 Ukey 详细逻辑图

4 整体流程图


跳转申请
常规申请
开放平台
路由参数限制
订单界面
路由，viewToken 限制
选中 Ukey
仅限当前私有化系统的 ukey
可获取详情信息
选择 Ukey
插入 Ukey
契约锁 ukey
支持其他系统 ukey 变更
仅 PC 支持
填写信息
如果有章面，确认变更
确认价格
提交订单
主体认证
未认证
主体授权
非本人
契约锁支付
平台方支付
烧制证书
初始化 Ukey
(后端)
清空 Ukey
初始化 Pin 码
(驱动)
初始化 Ukey
已申请
开票
申请证书
(后端)
申请证书
成功写入
(后端)
写入证书
写入图片
(驱动)
下载证书
(后端)
写入证书
订单完成