编辑导语：支付认证方式是支付业务的核心部分，一个银行通常有多种认证方式来应对不同用户的需求，如何向用户传递清晰简单的认证方式以及引导用户高效的完成认证操作是很重要的。本文作者为我们介绍了银行支付鉴权的定义、银行支付鉴权与认证方式的关系以及如何开展银行支付认证的鉴权体验设计，希望看后对你有所帮助。

支付认证方式的鉴权内容是支付业务中的核心业务逻辑，通过了解鉴权背后的逻辑将有助于加深对支付认证的理解，设计师应在充分了解一个支付方式背后鉴权的业务逻辑，才能更好地开展相关设计，让鉴权过程变得更加简单，体验更加流畅。

1. 银行支付鉴权的定义

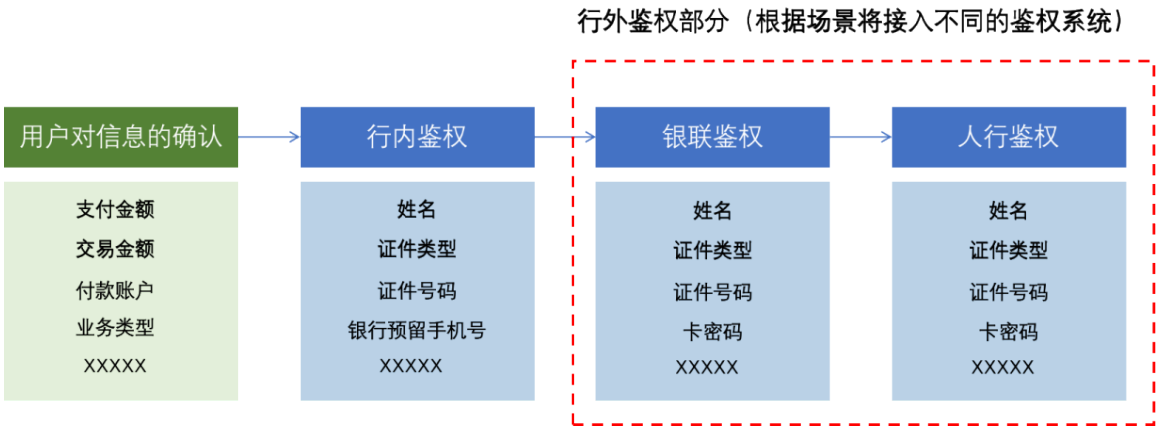
鉴权，从本质上理解是指验证用户是否具备访问系统的权利。银行支付鉴权则主要包含两个内容：用户对支付交易的授权和银行对用户身份的验证。

用户对支付交易的授权，是指用户对当下正在发生的支付行为中的信息进行确认并授权银行对其身份进行验证的操作，支付信息可包含但不限于支付环境、支付金额、交易对手、付款账户以及业务类型等。

而银行对用户身份的验证则是指银行对能代表用户身份的信息进行验证，验证通过后，授予用户访问相应的后台系统并发生后续扣款行为的操作；对用户身份的验证通常会需要采集用户的身份证信息、账户信息以及银行预留手机号等关键信息要素。

正对扣款账户的类型不同，又可分为行内鉴权和行外鉴权两种方式：

行内鉴权：是指扣款账户为本行账户，银行只需要通过行内自有的鉴权系统对用户完成身份的验证即可。 行外鉴权：是行内鉴权的延伸方式，在通过行内鉴权后，将采集到的信息按要求报送到指定系统进入下一环节的鉴权，这种方式通常用于扣款账户是他行账户的支付场景中。若扣款账户为本行账户，通常只需进行行内鉴权即可。



2. 银行支付鉴权与认证方式的关系

说到支付鉴权，则必须要提到支付认证概念。

从广义上理解，支付鉴权就是一种支付认证方式。

但由于支付鉴权通常面向用户所采集的信息过多，输入操作过多容易造成支付失败，因此银行通常在某种鉴权系统首次接入时，除了按系统要求让用户输入全量鉴权所需的信息外，还会给用户开通一种更为便捷的认证方式，给予用户一把“钥匙”。

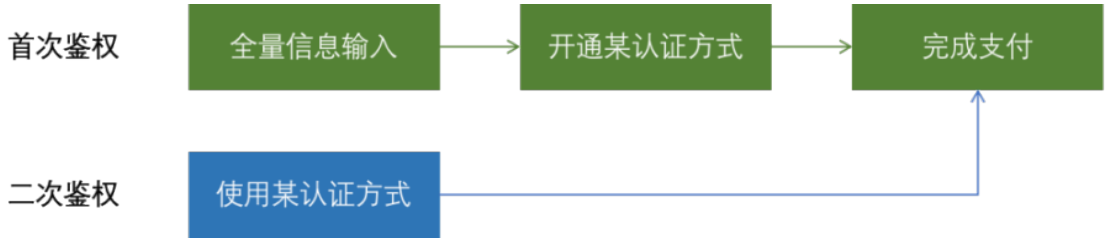
后续用户在再次接入该鉴权系统时，只需使用那一把“钥匙”即可视同输入全量鉴权信息。

那么这把“钥匙”就是我们通常理解的“认证方式”，如短信验证码、数字静态密码、动态密码器以及 U 盾等多种认证方式。

因此支付鉴权与认证方式的关系正如那全量鉴权信息与那一把“钥匙”的关系，通过使用某认证方式对用户完成验证来达到对用户全量鉴权信息的采集过程，最终完成对用户身份信息的验证。

因此，通常情况下，在首次对某种支付方式开通时，则会要求用户进行全量身份信息的输入并通过后台身份信息验证，完成支付。

在第二次支付时，即可使用已开通的支付方式进行认证（视同完成身份信息验证），无需用户输入全量身份信息，使得用户的支付流程变得更加便捷简单。



3. 如何开展银行支付认证的鉴权体验设计

那么面临着多种认证方式，银行该如何开展相关的鉴权体验设计呢?

本章节将围绕“简化用户授权”、“鉴权输入简化”、“鉴权流程轻量化”、“行内行外衔接”、“鉴权环境的安全感营造”五个方面来展开论述:

3.1 简化用户授权

应简化用户对支付信息的确认授权环节，尤其是要做好支付相关信息的优先级处理，突出关键信息，如支付金额、收款账户和收款对象，让用户快速完成确认。

在支付收银台中，用户需要完成的操作便是需要对当前支付信息的确认并授权银行开启对其身份的验证。

在支付信息的展示上，通常都会对支付相关信息的优先级进行处理后再向用户展示，对于其中的关键信息，如支付金额，一般都会是最为强调突出的信息，让用户对最为关键的信息进行确认，防止造成经济损失。

如中国银行的支付收银台上，对最终支付金额的展示进行视觉上和布局位置上的突出展示，让用户能第一时间对金额进行确认。

当用户对关键信息都确认没有问题后，即可授权银行开启身份验证（点击“立即付款”即视同用户同意授权）。

中行

付款详情

¥50.00

订单金额	人民币元 50.00
优惠	随机立减
订单说明	话费充值13
付款账户	长城电子借记卡 ( ) >

3.2 鉴权输入简化

在对用户身份进行验证环节中，在保证安全性的前提下，应尽量简化对用户身份信息的采集环节。

3.2.1 应尽量利用后台已留存的用户信息，减少身份信息输入量

通常在某些认证方式的开通过程中，会要求用户对身份信息进行详细的采集，在这种情况下，应充分利用银行后台前期是否已留存过用户的相关信息，若存在已留存过的信息，则不应向用户重复采集，尽量减少用户的信息输入，降低操作成本。

3.2.2 可利用设备特性进行简化手动输入

在对用户进行身份信息采集的过程中，可考虑采用设备特性来达到简化信息输入。

如当银行需要采集用户的账户信息（如银行卡号），要求用户进行绑卡时，可利用手机自带摄像头，运用 OCR 技术进行拍照识别，无需用户手动输入。

中行

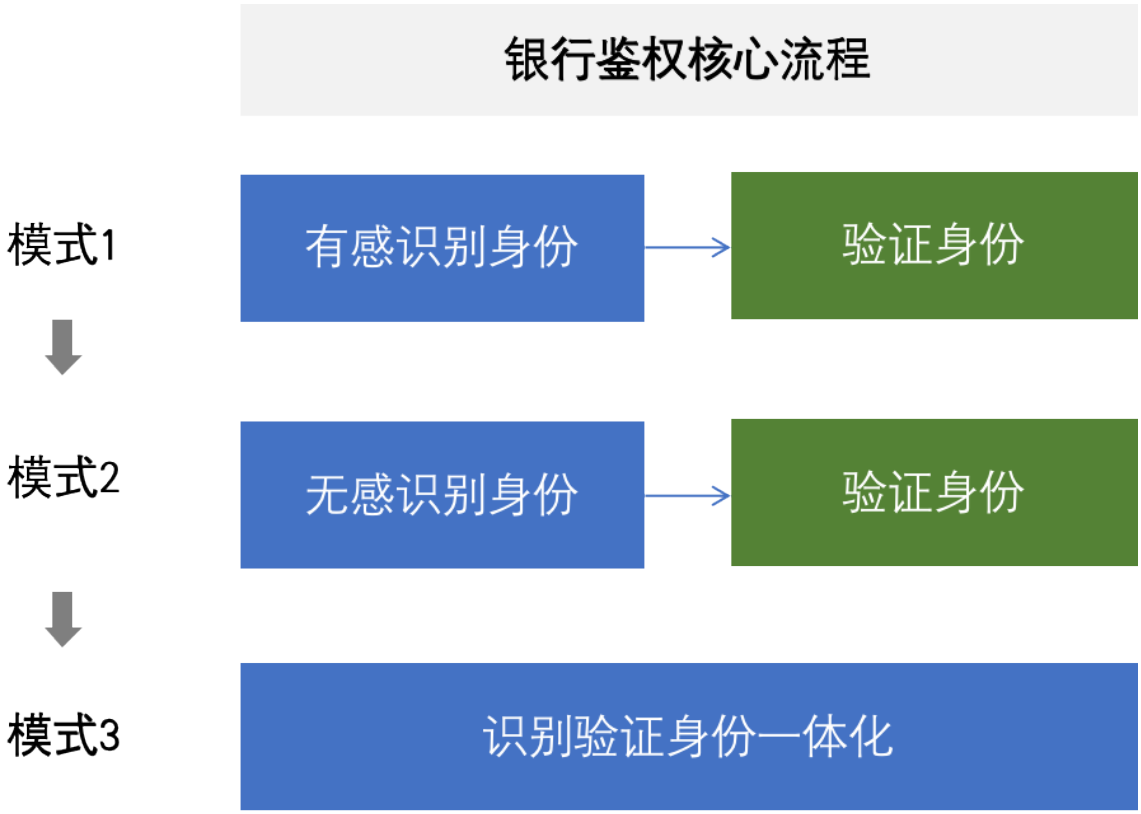

中国移动
23:35
27%
返回
关闭
开立电子账户
1
2
3
添加银行卡
验证身份信息
选择网点和设置密码
请提供一张本人一类借记卡，作为电子账户的绑定账
绑定账户
请输入任意一张银行卡号
拍卡
下一步

3.3 鉴权流程轻量化

将面向用户的鉴权流程简化，把复杂性留给银行后台。银行对用户鉴权的核心流程一般可分为识别用户身份和验证用户身份两个步骤。

识别用户身份是指在鉴权前，银行知道用户是谁；验证身份信息则是指银行验证当前操作确认是用户本人在操作。

二者是属于递进关系，通过识别用户是谁，再决定给用户以何种方式进行鉴权。而业界对于这个核心流程的处理通常有三种模式。



3.3.1 先识别，后验证：有感识别身份，再验证身份信息

在这种模式下，通常银行方在对身份信息验证前，会通过某些方式去识别用户是谁，先去判断用户是否具备进行用户身份验证的资质，如先通过让用户去进行登录来判断身份。

如用户在首次鉴权时，若用户不具备电子银行身份证，则会先让用户去开通；如用户未签署相关支付协议等情况，则会先让用户去签署。

通过这些有感的身份识别操作，让用户具备鉴权资格后，才让用户进入身份验证环节。

3.3.2 先识别，后验证：无感识别身份，再验证身份信息

在这种模式下，银行则会让身份识别这个环节变得轻量化，如通过前期的一些对支付设备的可信认证并通过相应的风险模型监控等。

当用户持有已认证的设备时（如苹果手机通过留存用户指纹来完成对设备的认证），即视同识别出用户身份，在支付鉴权流程中，只需对用户发起身份信息的验证即可，从流程上简化了鉴权，将识别用户身份操作从用户操作转变成银行后台操作，提高了支付效率。

3.3.3 识别验证一体化：识别身份和验证身份信息

在这种模式下，银行的目的则是为了最大化的提高鉴权效率，将身份识别和身份验证合二为一，比如运用人脸识别新技术，通过对用户的面部识别上同步完成了对用户身份的识别和验证，其安全级别可等同甚至要高于前两种模式。

对于用户而言，他无需进行多余的操作，只需要对准设别摄像头即可，大大的解放双手以及降低了操作成本，而银行则是将所有的复杂操作都留给了后台去处理验证，这种模式下的支付体验在现阶段看是较为新颖且最符合用户心理活动的（我无需证明我就是我自己），是未来下一代银行支付应去探索和对标的方式。

关于支付新技术的应用未来可尽量去利用用户的自然生命体征去展开探索，如通过可穿戴设备去记录获取用户心率、血型等去识别验证，通过声纹识别、瞳孔识别等用户身体特征去识别验证等，实现识别验证的一体化。

3.4 行内行外衔接：应注意行内与行外鉴权的相关衔接

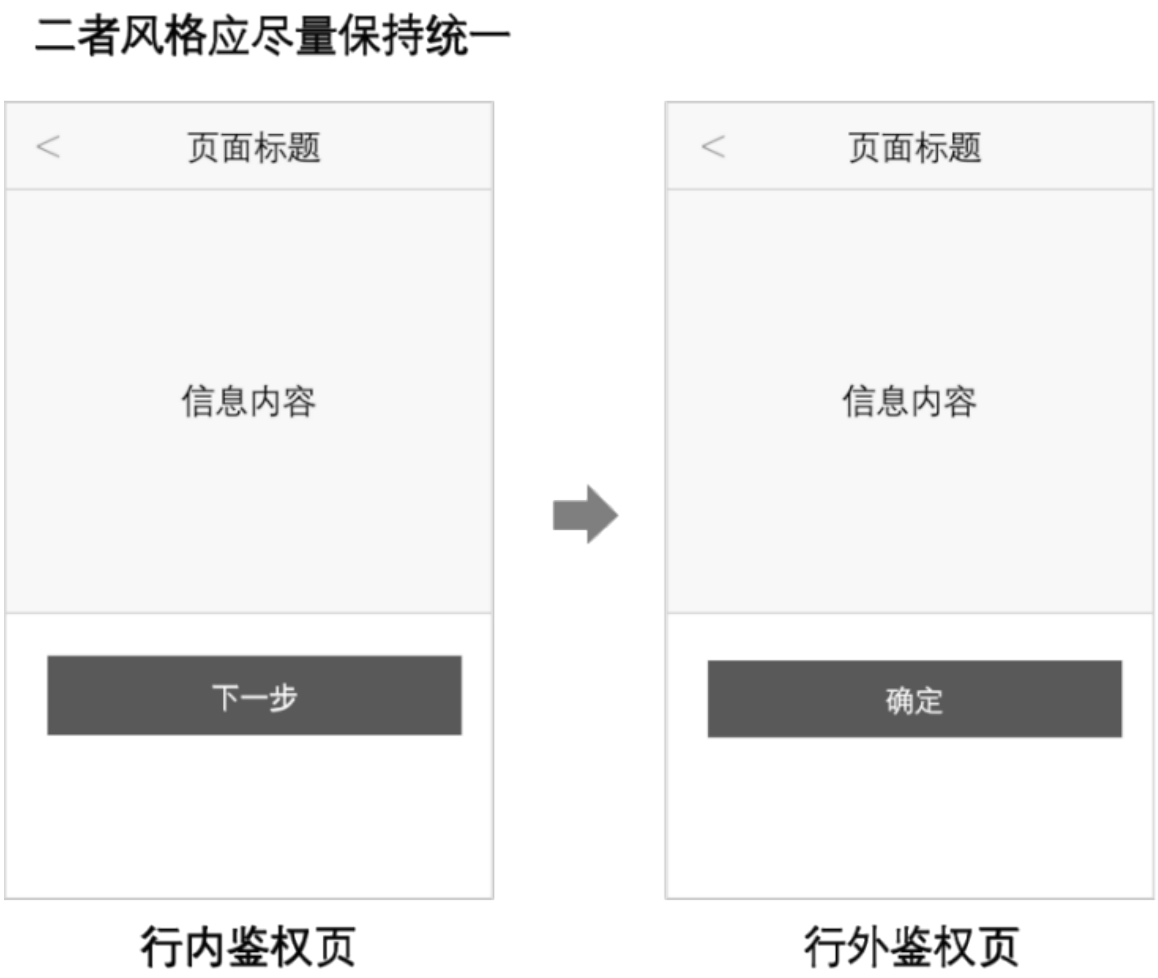
当某支付过程需要经过行内和行外多个系统进行鉴权时，通常推荐的做法是尽量让用户留在行内鉴权页面内完成所有身份信息的采集和验证，让行外鉴权环节通过后台系统无感完成，不发生页面的转场，不然容易导致用户流失.

但若是由于某些技术限制或安全原因，必须让用户前往行外鉴权页面上去进行对应的鉴权操作，则应当要注意做好行内与行外鉴权的衔接，保证体验流畅。

3.4.1 应尽量保持行内与行外鉴权页面的整体统一

3.4.1.1 应注意行内与行外鉴权页面视觉风格的统一

当用户身份信息经过多个系统去鉴权，需跳转到行外鉴权页面时，应尽量让行内外鉴权页面的视觉风格保持一致，避免给用户一种跳出原先行内页面的感觉，突然的风格变化容易让用户产生疑惑，如页面是否跳转出错了，从而增加用户的决策成本和操作时间。

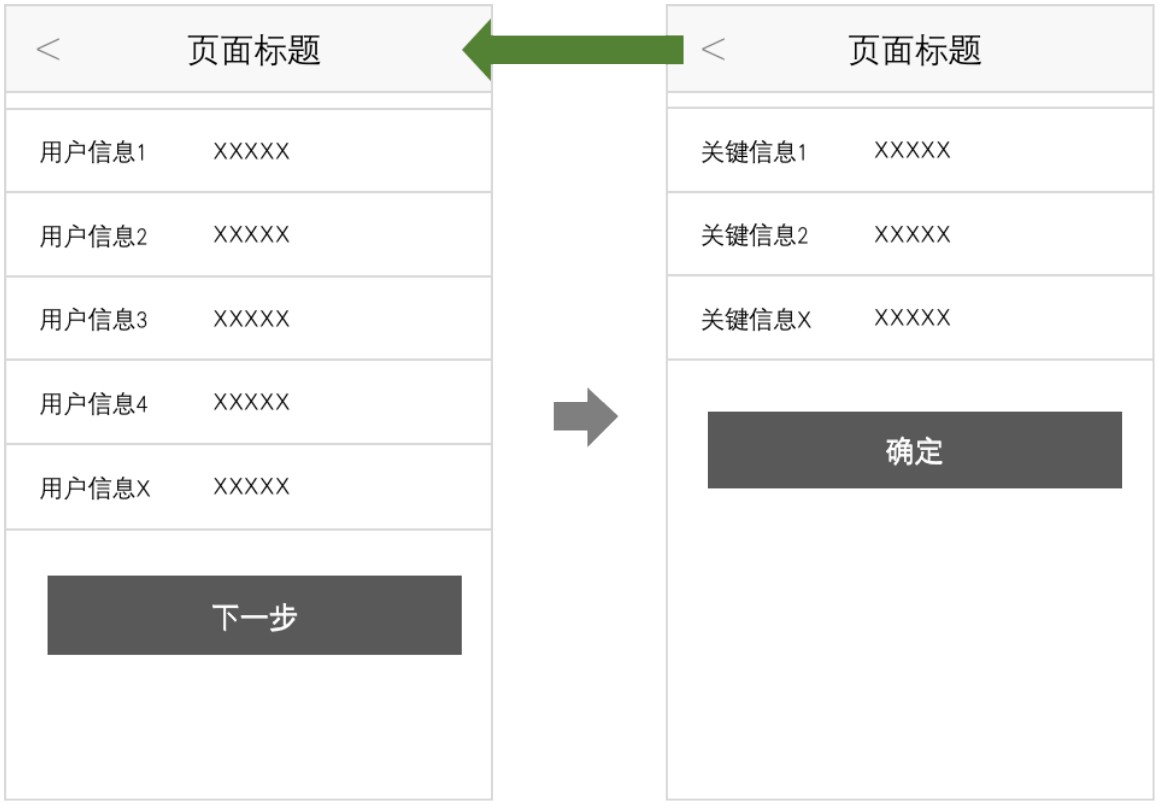


3.4.1.2 应注意对行外鉴权系统页面返回逻辑的合理处理

当用户从行内鉴权系统前往行外鉴权系统后，出于尊重用户的角度，应支持用户放弃当前行外鉴权环节，可返回至行内鉴权系统。

有些银行在行内鉴权页发生页面跳转至行外鉴权页时，则不再对用户在行外鉴权页上的操作进行跟踪，将所有的判断逻辑等都交予行外系统。

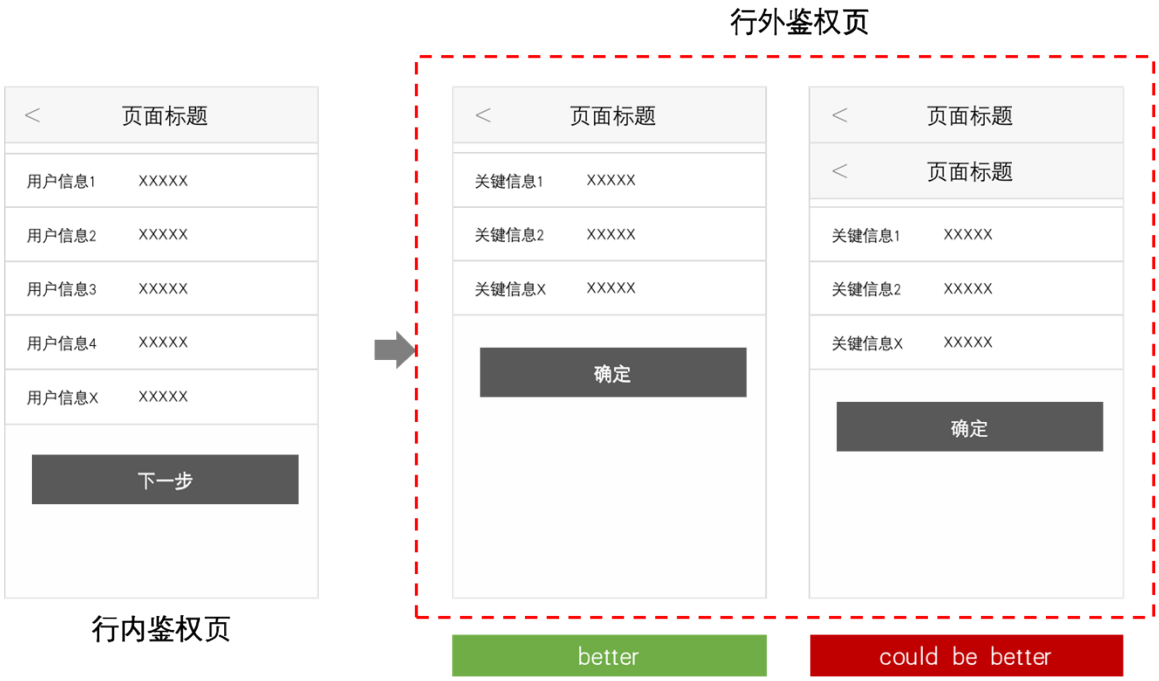
固然一些技术后台的逻辑判断因安全性等因素应当有行外系统进行判断，但对于“返回”这个基础性操作，应当要支持用户自由返回至上一个页面，而并非是按照行外鉴权页的返回逻辑执行，可能会返回到其它页面，导致流程跳出。



行内鉴权页　　行外鉴权页

3.4.1.3 应避免出现双导航栏模式

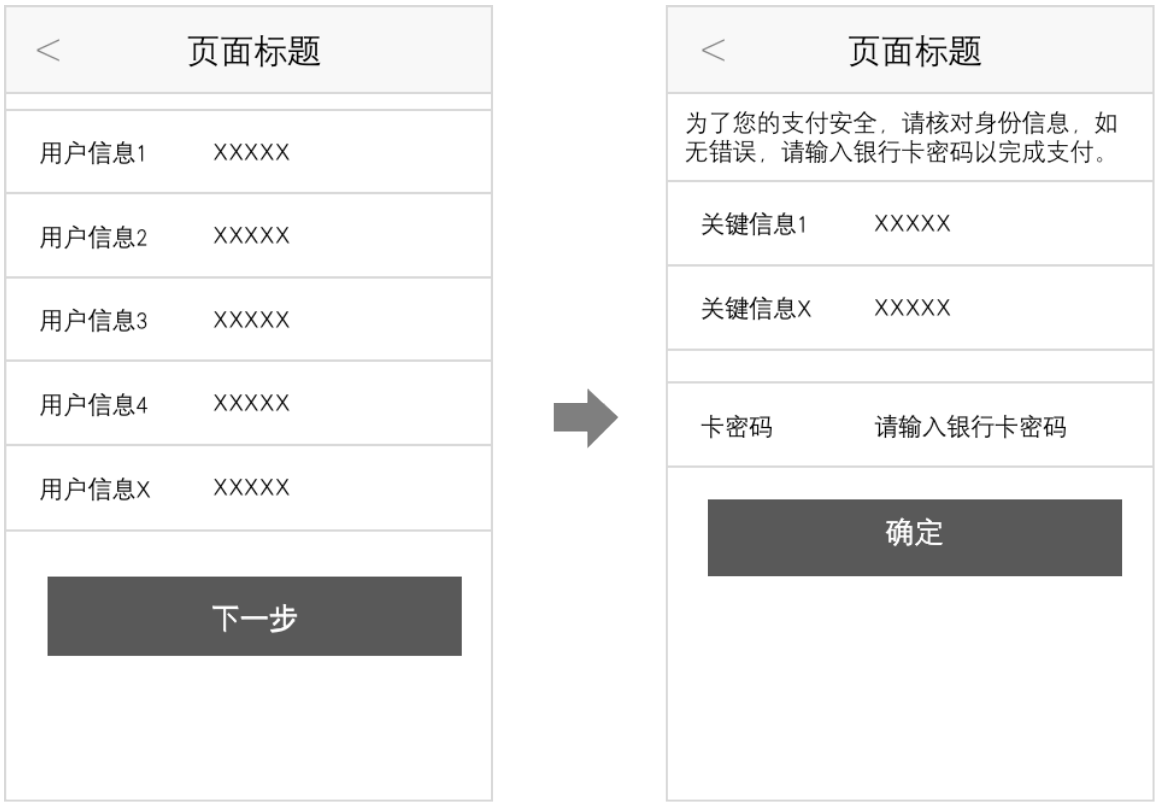
当用户从行内鉴权系统页面前往行外鉴权系统页面时，通常是通过行内应用浏览器打开行外页面，应注意避免出现双导航栏模式，造成用户认知混乱。由于两方页面通常由两方独立维护，应做好双方衔接的沟通，最终展示时保留一个导航栏即可。



3.4.2 应做好用户对当前支付交易的授权相关设计

当用户身份信息从行内鉴权系统发送到行外鉴权系统时，从安全性的角度出发考虑，应尽量在页面上展示关键身份信息，让用户快速确认，并进行友好文案的提示告知用户当前在进行的是什么环节。

如“为了您的支付安全，请核对身份信息；如无错误，请输入您的银行卡密码以完成支付”，通过关键信息的确认和文案提示快速完成用户对支付交易的授权确认，并进入身份验证环节。



行内鉴权页　　行外鉴权页

3.4.3 应对行外系统的反馈主动进行优化处理

在某些支付场景中，行内外的鉴权信息输入均可在行内鉴权页面上完成，那么关于行外鉴权后台系统返回的报错信息也会在行内鉴权页面上向用户展示。

那么很多银行在对行外系统报错信息的处理上过于简单粗暴，有时候直接将行外鉴权系统反馈回来的后台日志号码直接对用户进行展示，或者是将行外鉴权系统的报错对用户直接展示，但是这个报错提示对用户来说却是没有任何帮助的。

在这种情况下，建议银行应从用户角度出发，将报错原因进行分析处理，最终以用户视角来进行呈现表达。

如某支付场景用户采用了他行卡进行支付，则需从行内系统经过人行鉴权系统去验证用户身份信息，从人行返回的关于他行卡的报错是“账户状态异常（报错代码：7878332）”，但是这样的表述过于从后台技术视角阐述，对于用户无法直接理解，建议可主动对其分

析，并优化成“银行卡状态异常，具体原因请联系 XXX 银行咨询，客服电话：88888”。

通过这样的信息优化处理，让用户直观理解报错原因和后续解决办法，最终提高支付成功率。

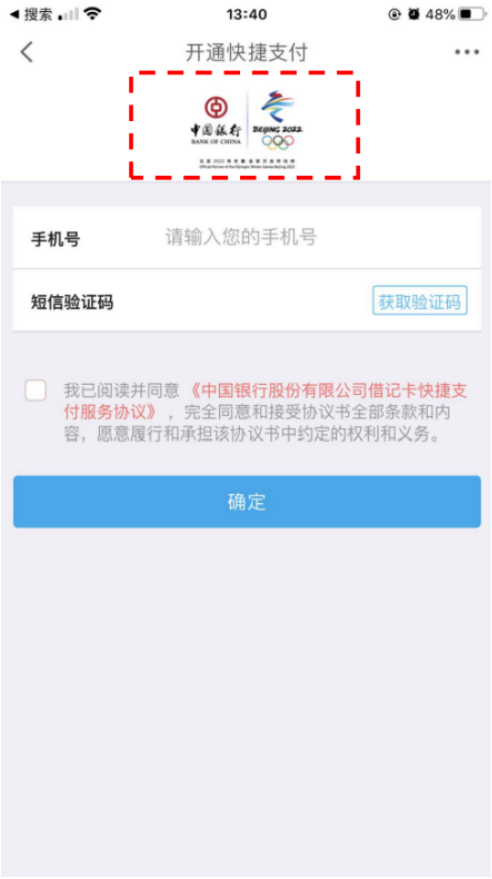
3.5 鉴权环境的安全感营造

应在整个鉴权环境进行安全感氛围的营造，给予用户安全感和信心，增强决策能力并提高支付效率。

3.5.1 企业品牌背书

在鉴权相关页面上可考虑将企业品牌进行直观展示，通过利用企业形象进行背书，增强用户对当前支付交易的信任感和安全感，才能放心地在当前页面将重要身份信息输入。

中国银行



邮储银行

3.5.2 合理信息告知

在用户身份信息输入的过程中，应对某些关键信息进行清晰到位的解释，让用户明白所输入信息的具体要求或用途，合理到位的文案提示告知将会增加用户对当前页面的安全感。

微信支付绑定新银行卡场景

邮储银行

3.5.3 页面品质感传达

在页面设计上给予用户品质感的传达将有利于增加用户的安全感。如果一个连页面设计都无法做到有品质感（如过时的风格、杂乱的布局等）的企业，那么用户将对其企业形象和能力产生质疑，进而对其支付产品的安全性产生质疑，从而降低信任度和安全感。

题图来自 Unsplash，基于 CC0 协议