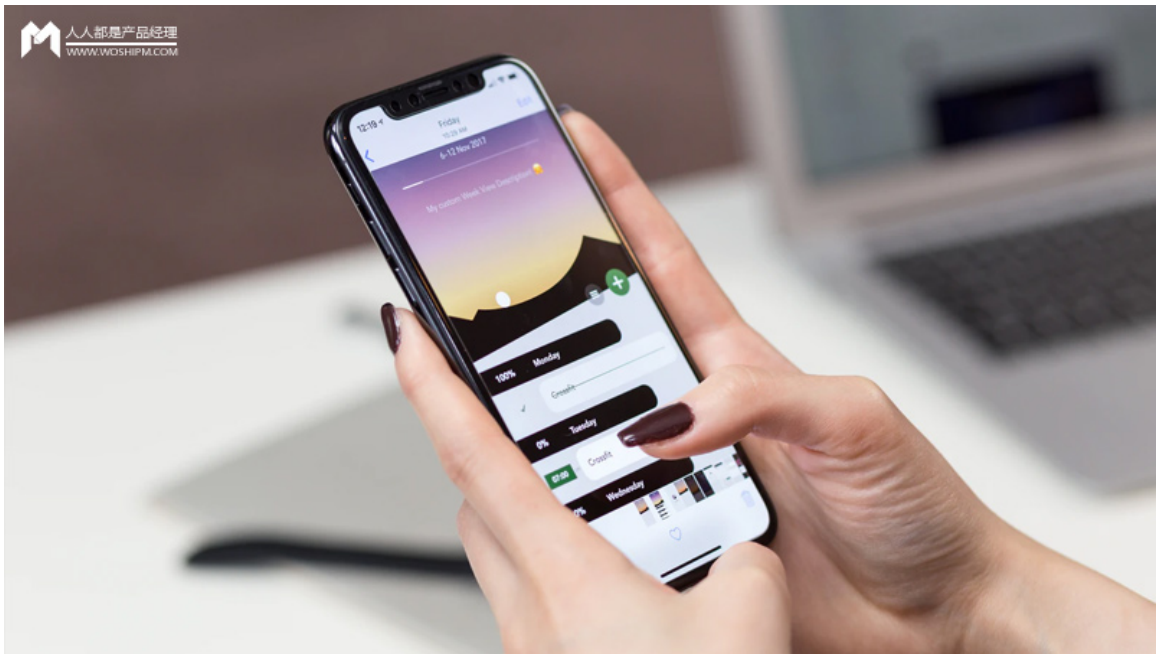
支付认证方式是支付业务中的核心部分，而一个银行通常拥有多种认证方式以应对不同的用户需求。在现实使用场景中，不同认证方式的展示形态以及使用方式等各不尽相同，尤其是在承接业务类型丰富的银行中，所拥有的认证方式往往可衍生出多种支付产品，那么如何向用户传递清晰简单的认证方式感知以及引导高效认证操作是极为关键的。



一、为什么银行会有多种支付认证方式?

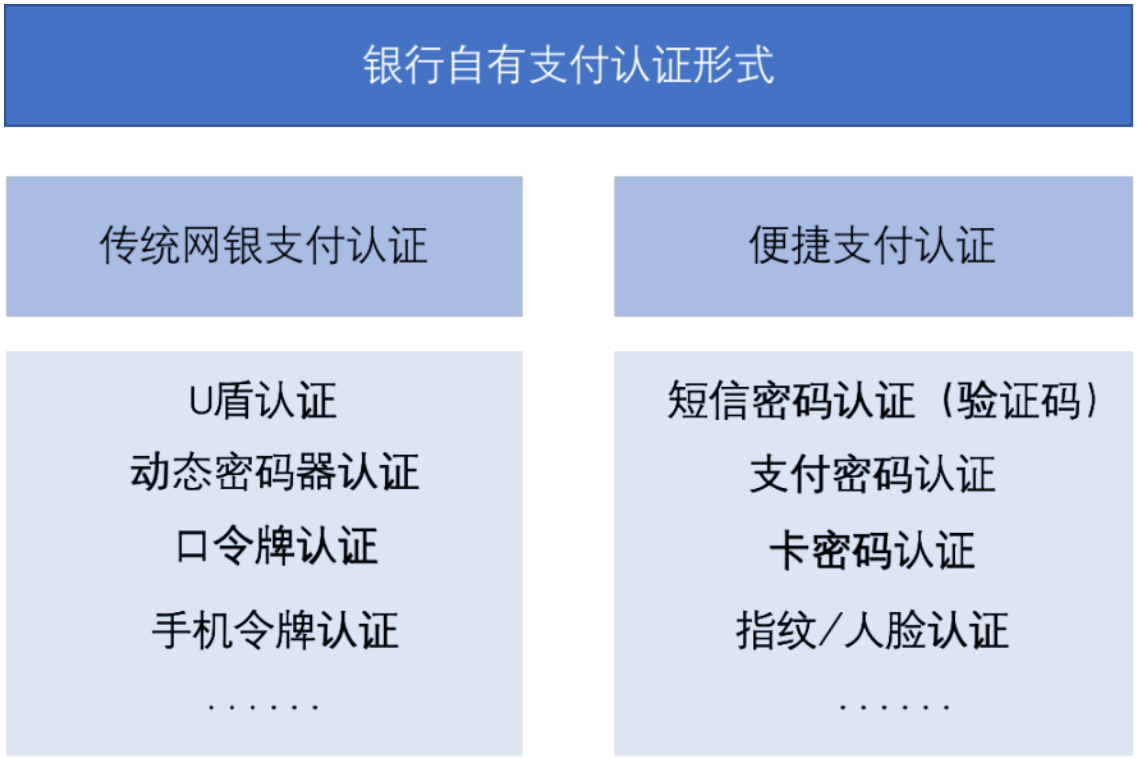
由于银行用户群体多样性强、导致用户诉求多样。例如在转账金额的诉求上，学生客户通常只有小额支付需求，动账资金通常在 1 万之内；上班白领则有较强的日常消费能力，动账资金在 2～5 万之间；小微客户的资金量则更大，会在 5～20 万之间；那么企业用户的资金动账量将会更大，可在数十万、数百万、数千万甚至更多。

因此由于不同用户的动账需求所涉及到的金额不同，随着金额的增多也就意味着支付风险的增高，因此银行在考虑便捷与安全性的前提下，提供了不同安全认证级别的认证方式以满足用户的多样诉求。

因此，为了满足不同用户的需求，银行自身通常拥有多种认证方式，一般可分为传统网银支付方式和银行便捷支付方式两个大类。

例如在传统网银支付方式中，有 U 盾、动态密码器以及口令牌介质认证等方式，而在银行便捷支付方式中有短信验证码（短信密码）、数字密码（支付密码）、指纹/刷脸等认证方式。

不同的支付方式所支持的业务场景和条件各有所不同，比如数字密码认证方式，作为银行主推的便捷支付方式，主流应用场景应是小额消费支付场景，其优点是便捷，缺点则是支付限额较低。而 U 盾这种介质类认证方式，因其本身安全性高的特点，所支持的支付限额高，但是缺点则是任务流程长且相对复杂，中间容易被打断，从而导致支付失败。



二、目前认证方式存在哪些问题?

因银行拥有多种认证方式，那么导致了对应产生的产品形态多样，有的是 U 盾（使用时需先插入），有的是短信验证码（使用时需先获取），有的是支付密码（需提前设置好），还有的是需要提前下载好某种安全插件并设置对应的密码等等，这么多样的认知形态、记忆成本以及操作方式，这些都容易让用户产生认知困惑和认知负担过重。

通常对于用户而言，支付认证中，他首先需要去辨识当前所拥有的认证方式，再开展后续认证操作。若他没有找到他所拥有的对应认证方式（如分辨不清楚本次要输入的密码到底

是哪个），那么极有可能放弃本次支付行为，将通过采用其它支付方式或渠道来完成；对银行来说，这不仅造成支付成功率低，也是对用户的支付服务没有做到位的一种表现。

且通常情况下，单一支付场景可支持多种认证方式，那么面对多种认证方式，用户不知道应该从哪个维度来决定最终的认证方式，用户可能会发问“这么多方式都有什么区别或特点”，“目前这种场景中用哪个最适合我自己的呢”等问题，最终在犹豫或长时间的选择中选定一种认证方式，其决策过程降低了整体的支付效率。

在支付认证过程中同样存在许多问题，因支付认证后台业务逻辑复杂，决定一个支付订单成功率高低的关键往往不取决于主流程的好坏上，而是在支付失败流程的如何及时补救和有效引导设计上。而在现实支付场景中，许多银行的支付产品往往让用户在失败的流程中无法继续支付，只能面对着冰冷的报错原因无从下手，最终放弃了当前支付方式的支付认证。

三、如何开展认证方式的体验设计

学会如何帮助用户去理解区分这些认证方式并引导快速完成支付相关操作则是本文要阐述的重点内容，主要围绕“形象认知简单”、“简洁布局一致”、“架构平级切换”、“流程模块通用”和“灵活反馈有效”五个方面展开介绍和应用说明。

（1）形象认知简单：应采用简单易懂的方式展示认证方式

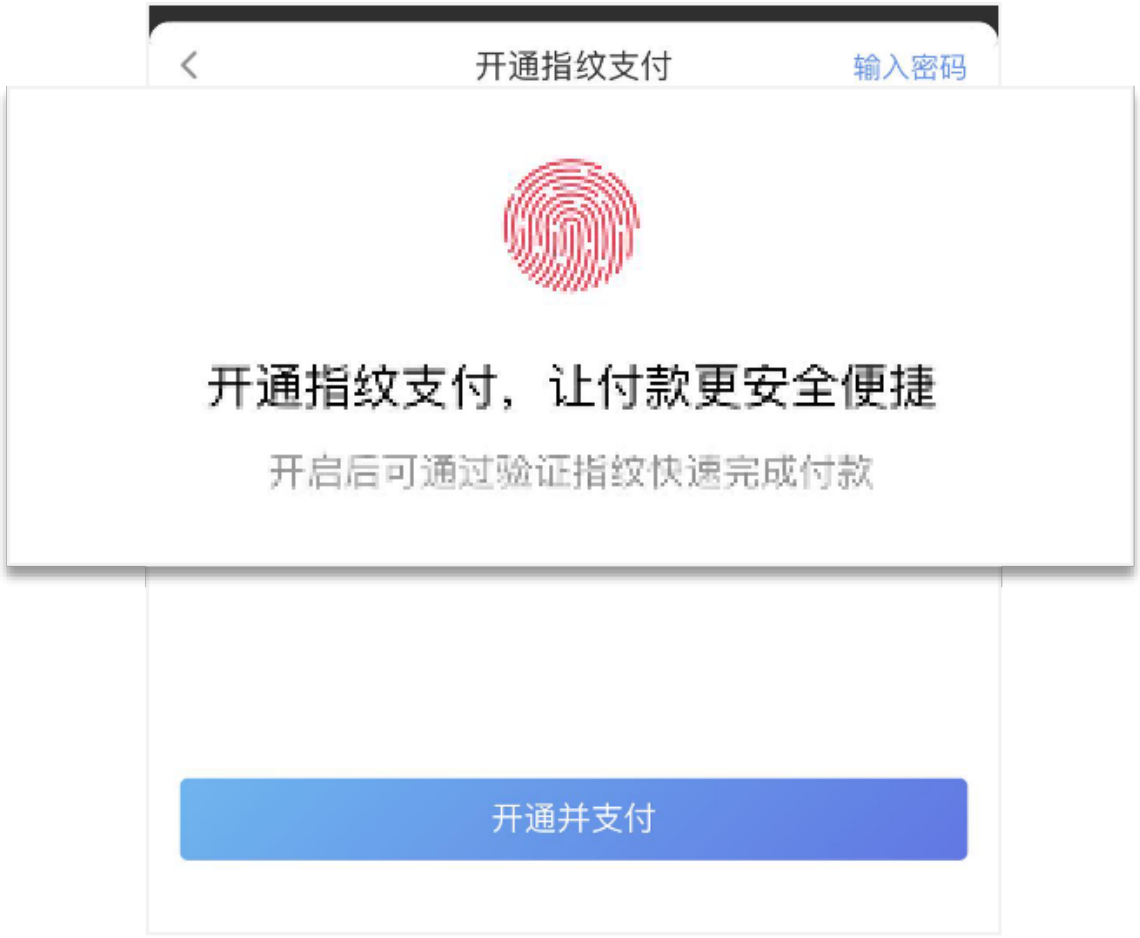
应采用直接明了、用户容易理解的话术名称来表达认证方式。有的银行推出认证方式的名称晦涩难懂，不但不利于用户快速记忆，也不方便开展业务营销宣传。

如农行曾推出“K 令”支付方式，而“K 令”这种表述是业务上比较专业的表述，而对于用户而言是无法理解的；实际上，“K 令”是一种依托物理介质（物理显示屏）展示的动态验证密码认证方式，其密码在使用过一次后就失效，下次再次使用时将重新生成新的验证密码。

在安全级别上要高于常规的短信验证码，支付限额也比短信验证码认证方式高，是为手机移动支付推出的限额较高的安全认证方式。因此当这个“K 令”表述向用户路由推荐展示时，用户或许会不明白其背后的产品逻辑和优点，从而产生困惑（如使用这个方式安全吗？），可能会去询问他人求证后再使用或者直接进行其它认证方式的切换，导致本次路由

推荐路径失败。建议采用较为通俗易懂的表述去命名认证方式，如“动态密码器”、“短信验证码”等符合大众认知的话术去描述。

应采用形象化的方式直观展现认证方式。可采用可视化形象表达出当前认证方式的形态，直接了当告诉客户是什么认证方式，让用户易于理解当前所采用的认证方式是哪种并提前做好准备。如当有新的认证方式向用户推出时，可考虑通过友好文案及可视化方式直观突出新认证方式的特点，可通过介绍对比不同认证方式之间的差异和使用流程，让用户快速掌握对新认证方式的理解和操作。



应对认证方式的优点、特点进行明显提示。对认证方式的优点进行表述，可增加用户操作的安全感和信心，如安全、限额高等。对于认证方式的特点也要进行必要提示，如短信验证码认证方式存在时效性，应在认证过程中对时效性进行提示，避免用户因自身原因导致认证信息输入缓慢导致验证码过期失效，最终造成支付失败。

用户感知

因此，当支付认证方式向用户展示时，应考虑尽量降低用户对其的认知门槛，以直观贴切的设计去引导用户快速进行下一环节，最终提高支付效率。

（2）简洁布局一致：各种认证方式在界面布局和关键操作方式上应尽量保持一致。

考虑到用户可能要在不同认证方式间进行切换或不同场景下使用不同认证方式进行支付，因此在各认证方式的界面布局上应尽量保持一致，有利于用户快速学习并提高操作效率。因为布局的一致也是为了给用户传递认知和相关操作体验的一致性。

如工行 e 支付在手机充值场景中，不同认证方式界面统一采用的是半浮层形式，这有助于用户对认证方式的认知保持一致，当用户面对这种半浮层样式，潜台词是告诉用户：现在要进行支付认证操作了。

因需要从多种认证方式向用户进行路由推荐，因此用户每次采用的认证方式可能会不尽相同，因此需要在页面布局上尽量保持认知的一致，告知用户哪些操作应该在界面上哪个地方去寻找，布局的一致性将保证用户在不同认知方式中的操作上趋于一致。

如工行 e 支付在认证方式的界面布局上，统一考虑了认证信息输入区域、键盘操作区域、切换认证方式区域等关键核心操作区域的布局一致性。其中，切换认证方式是每个认证方式中重要操作，它在界面布局上的一致能保证用户不管是被路由到哪个认证方式，都可以通过快速识别切换入口位置并找到他自己想要的认证方式，保证支付流程的不中断。

工行e支付—手机充值场景

（3）架构平级切换：在路由推荐认证方式中，应支持用户自主切换至其它认证方式，尊重用户的选择

考虑到用户习惯的原因，若后台智能推荐给用户的认证方式并非用户想要使用的方式，应支持用户平级切换到其它认证方式中去。在设计中应注意其它认证方式与当前智能路由方式在信息架构上的平级关系。因为虽然通过智能路由为客户推荐支付方式，但是并不代表不尊重用户，依然把最终的决定权交给用户。

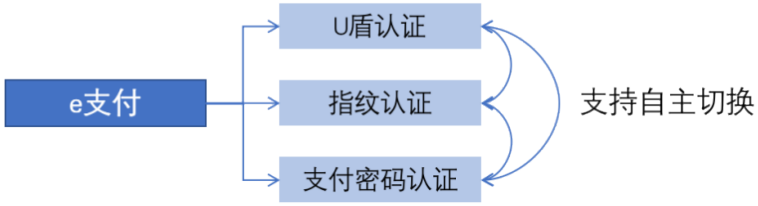
例如工行 e 支付在转账汇款场景支持多种认证方式，在智能路由推荐规则下，推荐了 U 盾认证方式，若用户此时不想采用 U 盾认证，可直接选择其它认证方式进行验证。

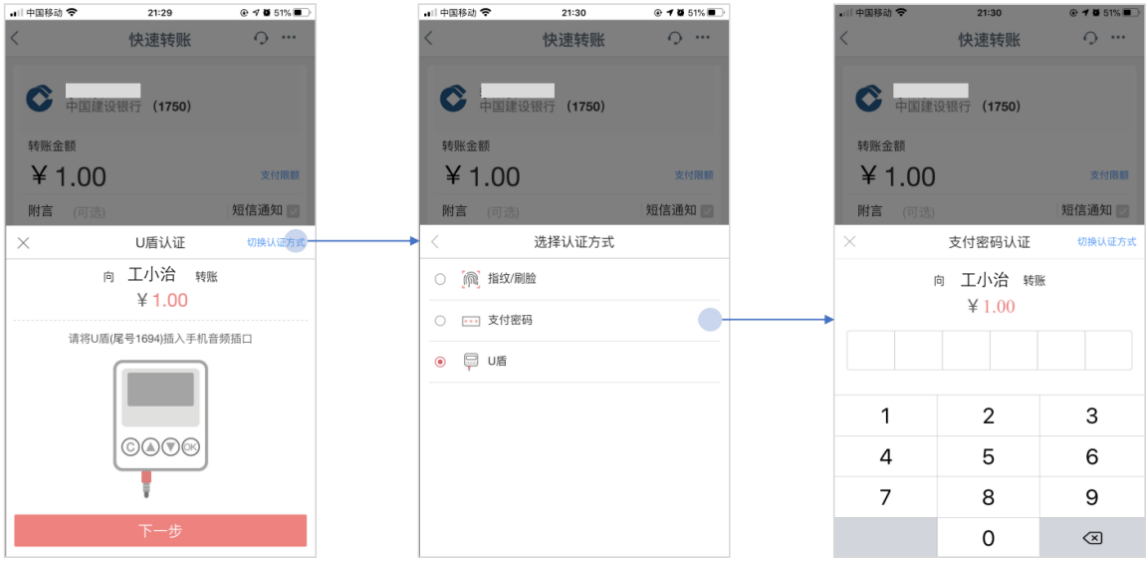
如招商银行，在某个话费充值场景，推荐客户使用指纹认证方式开通并支付，若用户不想采用这个方式，可切换至支付密码方式进行支付操作。同时可以在后台系统里记录下用户的选择，在下次同类型的支付场景中便可为用户推荐相同的认证方式。

如在当下疫情防护期间，用户在日常出行中必然是带着口罩，而在这种特殊时期的支付场景中用户显然是不方便进行刷脸认证的，但是在日常消费支付中，仍然有不少支付产品依然给用户推荐刷脸认证方式，那么用户则需要每次手动将刷脸认证切换为密码认证，增加了非必要的操作动作。这不仅在用户习惯上没有去尊重用户，也不符合疫情期间所推行防护理念。

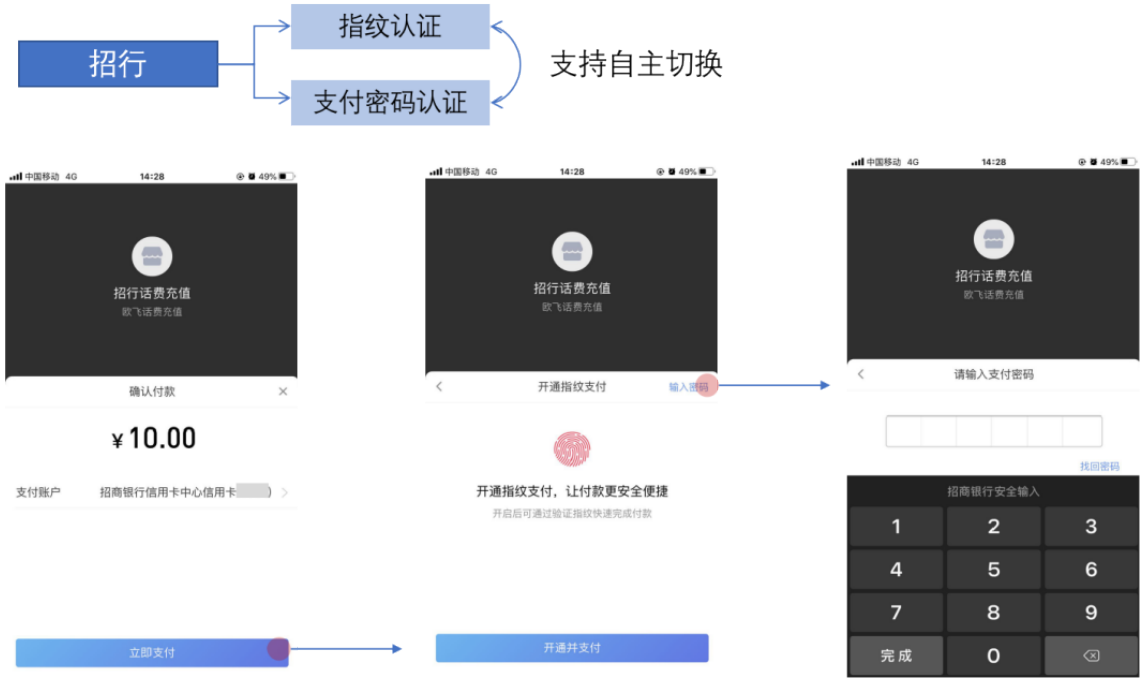
如果可以结合用户的定位地点（如在室外）以及用户在室外进行的支付操作行为（如切换成密码操作），那么下次再为用户进行推荐认证方式时，则应要为用户推荐上次所选择的认证方式，而不再是一味推荐刷脸认证方式。

工行e支付-转账场景





招行-话费充值场景

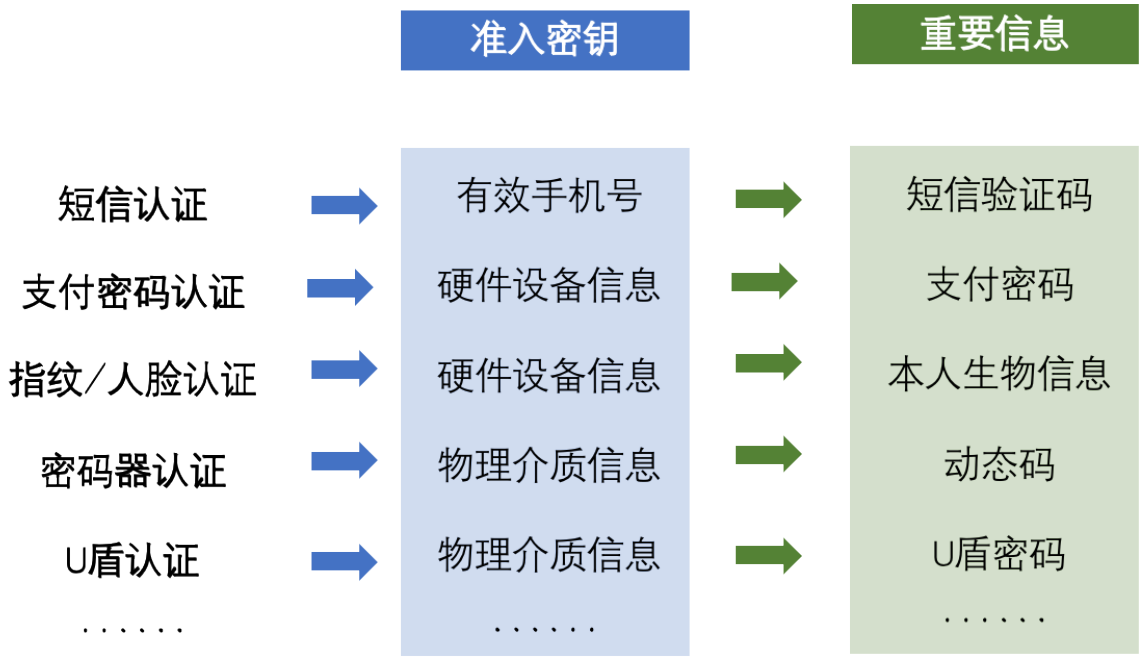


（4）流程模块通用：应做好认证流程中的通用模块设计且保证流程一致从而提高操作体验的一致性和流畅性

虽然不同认证方式的任务流程各不相同，但为了保证操作体验的一致性，应尽量提炼流程中的通用模块或调整某些认证方式的任务流程以求最终达成一致的任务路径模式，最终使得用户在使用各种认证方式时任务流程是一致的，降低学习成本从而提高操作效率。

在认证流程中，关键认证通常包含“准入密钥”获取和“重要信息”验证两个步骤。二者是属于递进关系，必须先获得“准入密钥”，才可以进行“重要信息”的验证。

如短信验证码认证流程中，“准入密钥”是有效手机号（当前正在使用的），“重要信息”则是发送到手机号上的短信验证码。如在密码器认证流程中，用户需要先持有“准入密钥”（密码器），才可以进一步将密码器上的动态码（重要信息）输入到支付界面中去进行验证。如在支付密码认证方式中，“准入密钥”实际上是后台自动获取到当前支付所使用的设备（如手机）是否为原先开通支付密码时所绑定的设备，只有通过获取到设备号（IMEI）即“准入密钥”，才可以进行 6 位支付密码的验证步骤。



因此对于体验设计来说，应做好“准入密钥”获取和“重要信息”验证的衔接环节，让两个步骤不中断从而保证流畅的认证体验。为了能提高操作效率，最好是能将两个步骤无缝链接。

例如短信认证方式中，通过向用户前期开通时预留的手机号发短信，无需用户手动输入手机号并点击获取。例如支付密码认证方式中，后台将自动发起对当前支付设备进行设备信息检索，若获取到所绑定的设备信息，则直接进入支付密码验证步骤。

在两个步骤的衔接当中，可通过文案提示、可视化形式等多种形式进行有效引导，尽可能保证流程不中断。如在短信验证码认证中，可提示用户是向哪个手机号发送了短信，以便用于去查询。如 U 盾认证需要先将 U 盾物理介质插入手机中，可通过可视化方式进行提示，有效进行了“准入密钥”和“重要信息”的衔接。

建行

工行

（5）灵活反馈有效：应对认证结果进行及时有效反馈、可结合场景来选择反馈的形式并提供后续引导操作

1）若支付认证通过，认证结果为成功状态。应将关键支付信息展现给用户，可包含交易对手、交易金额、到账时间以及其它相关信息展现，给予用户清晰明确的成功提示确认与后续引导操作，如查询订单。

招行

2）若支付认证不通过，认证结果为失败状态。应尽量将准确失败原因及相应后果告知用户，并继续引导用户完成支付操作

若当前失败原因对当前认证方式的有效性不造成影响（用户可继续使用该支付方式进行支付），应尽量在不打扰用户的原则上去提示用户。让用户在轻提示中继续完成支付流程，提高支付效率。

可采用一些对用户打扰较小的交互反馈形式，如随行提示，toast 提示，无需用户对当前失败原因进行确认，可直接进行再次输入，简化流程。不宜采用如弹框此类的样式，对支付流程打扰较强，增加用户的操作成本。

支付宝

better

对支付流程打扰小
随行提示–轻提示

招行

could be better

对支付流程打扰大
弹框提示–重提示

若当前失败原因导致当前认证方式失效（如多次因密码失败导致当前支付方式冻结），应进行清晰提示并支持切换使用其它认证方式，以便支付流程不中断。

总结

以上便是通过五个方面去描述如何开展支付认证方式的体验设计，相信通过做好认证方式的认知表达、布局及相关引导操作、流程模块通用设计和灵活的有效反馈对用户完成支付认证流程有提升操作效率的作用，从而最终提高支付产品的整体体验。