OliverWyman 奥纬咨询 | ibfed International Banking Federation

数字信任

银行如何保障数字身份安全

中文版翻译

中国银行业协会 CHINA BANKING ASSOCIATION

Marsh GuyCarpenter Mercer OliverWyman

国际银行业联合会前言

现在，许多日常活动都依赖数字服务，包括实时新闻和网上购物等实用服务，以及医疗保健和银行业务等关键服务。随着人们愈加依赖数字渠道来维系最重要的关系，数字经济中对身份的识别变得比以往任何时候都更为重要。

虽然人们对数字业务的依赖性不断加大，但全球各地的数字身份框架很大程度上仍然需要依托于模拟和纸质证明。例如，我们能够与身处地球另一端的医生交谈或通过点击一个按钮立即汇款，但当需要证明我们的身份时，却通常需要上传一张往往是多年前签发的纸质文件照片。

在全球各国和各地区政府和公共部门共同、积极地推动下，不久的将来我们可能不必再运用上述传统、纸质的数字化身份来证明自己的身份，而是广泛采用数字化身份凭证，以更便利的方式来证明自己的身份。

在身份数字化进程中，银行得益于客户身份验证能力这一核心竞争力，天然地处于发展数字身份计划的核心。例如，强监管使得银行能够可靠地保存客户最敏感的数据；又如，银行在获得每个新客户时，必须通过一个被称为“了解你的客户”（KYC）的程序识别和验证客户身份。

数字身份计划实施有望，但也必须谨慎管理。数字身份计划能够切实减少诈骗活动并催生各种新产品和服务。与此同时，数字身份也可能会对全球市场产生深远影响，并引发隐私保护、普惠金融和政府角色等方面的重要问题。希望本报告能开启有关这一关键领域未来发展的热烈讨论。

Rob Nichols
国际银行业联合会主席、美国银行家协会主席兼首席执行官

中国银行业协会前言

近年来，随着各类数字网络基础设施和应用的不断发展，数字网络空间对人民生产生活、经济运营、国家治理和国际政治形势产生了重要影响。在不同的数字网络空间中，可信网络空间已经成为国计民生的重要保障，也是国家信息化战略的重要组成部分。数字身份（在我国又称“网络可信身份”）是可信网络空间的必要构成，是居民、企业和机构远程交流、交易和事务办理的关键基础，在疫情期间和未来万物互联的时代更是如此。“实施网络可信身份战略”已成为国家网络安全的重要战略，此外个人身份信息的合理收集、保存和共享也是近年来网络安全与消费者权益保护的重要议题。

在国家实施网络可信身份战略和强调个人信息保护的浪潮下，银行作为接受严格监管的金融机构，在过去运营中积累了丰富的客户身份收集、识别与验证及可靠的信息存储与交换的经验，具备生成和交换可信身份的技术，能够提供消费者身份及金融数据的充分保护，有基础、有能力成为数字身份生态体系的重要成员，甚至可成为提供相关数字身份的服务机构。

以何种身份参与数字身份生态体系是银行重要的战略命题。这不仅将给银行带来潜在的新收入，更给银行带来了重塑客户旅程，以“客户为中心”开展业务的战略机遇，但同时也意味着长期的资源投入和潜在的各类技术应用风险。整体看来，银行业需保持行业协作，积极参与政策及标准制定，支持国家网络可信身份战略的实施，保护消费者数据隐私权益，促进金融普惠和数字普惠。

本报告从全球视角，全面总结了当前全球各国数字身份体系发展情况和数字生态体系的必要构成，同时对银行以何种角色参与数字身份生态体系这一命题进行了探讨。希望能抛砖引玉，开启中国银行业未来如何参与数字身份生态体系建设的讨论。

邢炜
中国银行业协会党委书记

奥纬咨询前言

随着数字互动在人们生活的各方面开始发挥着越来越关键的作用，消费者亟需可靠、可信赖的数字身份证明，上述需求迫切到需要在未来几年内得到满足。

很多国家和地区都已经陆续通过公共部门或私有部门采取了行动来满足上述需求。印度、新加坡和爱沙尼亚已通过公共部门开展数字身份计划，北欧国家和加拿大也已经推出了相应的私营部门计划。中国和比利时的数字身份生态系统已涌现出了两种或两种以上的不同的数字身份计划。

身份数字化转型预计将给社会、金融、经济等诸多领域带来深远的影响。我们正在开始理解其影响，包括如何向消费者提供数字身份相关服务、如何确定数据所有权、如何确定营销关联获得最终消费者，以及数字身份服务行业的结构等，上述转变甚至可能重塑居民、政府和私营部门之间的关系。

开发数字身份必然是一项复杂的工作。无论采用何种交付模式，都需要政府、银行业和其他多个部门之间的紧密合作，包括创建信任框架、建立生态系统、开发应用场景和解决方案，以及扩大数字身份的应用等。银行想要在数字世界中保持相关性，就必须在转型中发挥关键作用。

我们很荣幸与国际银行业联合会合作、中国银行业协会共同推进本项重大议题。我们相信，数字身份不仅会改变我们的生活方式，更会开创银行业的新时代。

Ted Moynihan
奥纬咨询 执行董事合伙人

目 录

执行摘要

驾驶证、护照、出生证明……这些政府颁发的实物凭证历来都是银行业及其他领域个人识别流程的核心。而现在，数字身份计划为我们提供了非常有效的替代方案，能够帮助我们验证个人信息并与政府部门、银行、用人单位和其他组织分享个人数据。

有了数字身份认证，机构可以授权支付、完成客户身份识别与验证（KYC）、开立账户、管理应用程序的访问权限、提供证书、维护供应链安全，甚至完成背景调查。如今社会充斥着大量数字互动，导致个人信息碎片化、诈骗手段升级，而数字身份可以帮助我们应对这些重大挑战。

国家数字身份计划（National Digital Identity Scheme）是对数字身份最有效的利用。经验证明，国家数字身份计划能够将相关技术系统和协议整合为一个简化的身份认证服务，从而消除消费者和企业之间的摩擦，同时还能提高双方互动的安全性。虽然目前建立了国家数字身份生态体系的国家还不多，但对于这个问题，我们已经有了几种不同的参考做法：政府主导、私营部门主导和二者混合主导的数字身份计划。除了那些已经开始着手建立数字身份的国家以外，美国、英国、巴西、日本、澳大利亚、南非和欧洲各国等许多国家也有可能在未来十年里加入此行列。

从当前实践看来，一些国家数字身份计划甚至并非由政府主导，而是由银行主导。对于那些有意在国家数字身份生态中发挥更大影响力的银行来说，它们也可以借鉴相关经验。

国家数字身份计划的引入为银行的客户带来好处。银行在日常工作中已积累管理大量个人数据和验证庞大客户群体身份的经验，并且银行之间大多构建了保障网络和信息安全联盟。因此，如果银行能参与制定国家数字身份计划，可以使得消费者更加信任该计划的稳定性和安全性。此外，参与制定国家数字身份计划也会为银行提供诸多好处，例如能够降低运营费用、减少欺诈风险、改善客户对银行的观感和忠诚度，还可能带来新的收入。

随着数字身份信息更加丰富，用途更加广泛，如果银行能提供这种服务，就相当于抓住了一个为客户规划服务，同时还能改善端到端客户旅程的战略机遇。尽管这项服务会产生一定研发成本，但据估计，数字身份服务机构仅从“身份验证”这一项业务中就可从每位客户获得每年40美元的收入。

对于那些目前还没有建立好全国性的数字身份生态体系的国家来说，重要的问题还包括如何确定实施路径，例如银行应该成为该体系的领导者还是参与者。道德层面的考量和如何促进金融普惠与数字普惠将是国家关注的核心。引入数字身份系统既可能促进金融和数字普惠，也可能适得其反。国家应确保有更多的人在开始使用数字身份时能得到相关引导，这样便可以缩小数字鸿沟。

如果使用得当，数字身份能让所有互动变得更简便、更安全，同时还会提高居民进行数字活动时的安全感，让他们在日常生活中更愿意信赖银行。

1. 数字身份的前景展望

数字身份计划致力于为人民提供一种更为简单、安全的方式来获取和使用线上和线下服务。目前已推行数字身份计划的国家不多，当前所有计划均由政府和/或私营部门主导。其他很多国家也正在制定相关计划，并确保在未来十年内制定完善。

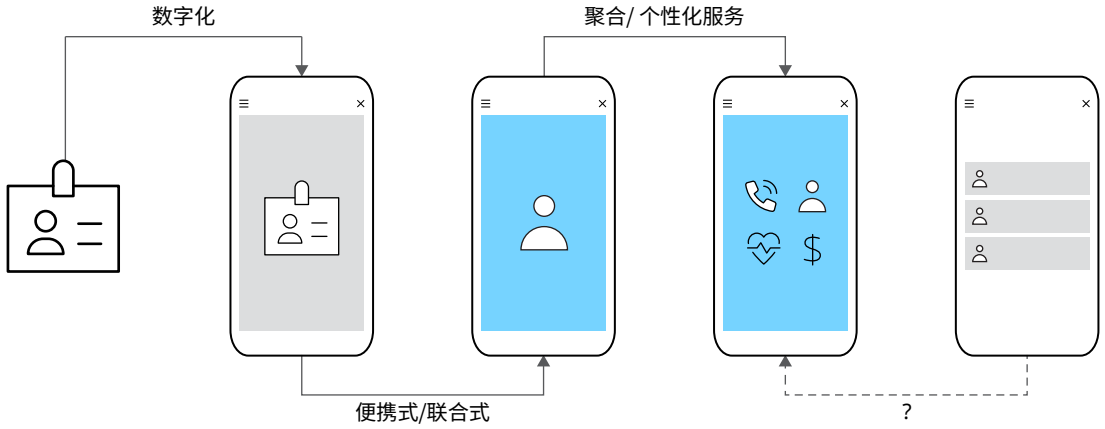
数字身份的形式

在全球范围内，互联网用户拥有多种登录方式，以获取从社交媒体到银行等各类线上服务。关于数据安全漏洞和个人数据滥用的案例比比皆是，很多人都头疼该如何保障网络和身份信息的安全。国家数字身份计划能够取代实物形式的身份识别及零散的数字身份，为消费者提供更安全的管理和控制个人数据共享的手段。

数字身份存在多种方案。最简单的是实物身份凭证在数字化流程中的应用，例如在开设网上银行账户时，使用经政府服务机构等方式认证的文件扫描件。高级一些的是，多国政府发布了数字化的“电子身份证” 身份凭证（e-ID），居民可以凭借它们来验证自己的身份。如果再高级一些，则是单一的、集成的身份关系（业内称为“联合”身份模式），可以帮助居民在访问各种第三方服务或产品时验证身份，从而在流程上为消费者提供更为流畅无缝的服务体验。

图 1: 数字身份凭证的形式

			数字身份（由政府或私营部门运营）		
	政府签发的实体身份证	**政府签发的电子身份证**	**基本数字身份**	**集成数字身份**	**单点登录**
采集的数据内容	核心个人数据（姓名、出生日期等）	核心个人数据	核心个人数据	核心数据以及交易、健康、教育背景等数据（子集）	发行人持有的数据（子集）
数字用途	一种实体证件，扫描后进行数字登陆	一种用于执行（经许可的）数字访问的数字凭证	一种帮助用户以数字方式验证或分享个人数据的服务	与基本数字身份一样的用途，并允许选择性验证和分享更多核心数据之外的数据，能实现数据聚合和个性化服务	一种帮助用户开通数字身份并提供（未经验证的）信息的服务
数据最小化	否	否	是	是	是
示例	无	• 中国（政府签发的身份证） • 爱沙尼亚（电子身份证） • 比利时（电子身份证） • 日本（个人编号卡）	• 中国（钱包） • 爱沙尼亚（智能身份证） • 比利时（itsme） • 北欧（BankID） • 欧盟（拟议钱包	早期拓展功能： • 中国、比利时（身份证显示新冠相关信息） • 加拿大（Verified.Me 财务数据）	使用……登录



来源：奥纬咨询分析

数字身份计划并非总由政府或公共部门提供服务，私营部门也可以运营。例如在挪威，很多人所使用的“BankID”就是由当地银行旗下的一家商业实体公司运营的。它能够帮助客户在抵押贷款申请过程中摆脱纸质文件，将抵押贷款申请过程缩短到一天[1]。消费者服务和用户旅程正经历重新设计并受益于数字身份计划。数字身份能确保所有用户都能访问相关界面，并保证客户需做出重要决定时不会面临不必要的麻烦且能享有充足的考虑时间。数字身份不仅能够提升消费者抵御恶性网络活动的能力，也给对网络安全持怀疑态度的消费者带来了信心。

数字身份生态系统可利用评分系统（或“保证等级”）划分身份验证的可信度。评分基于一系列技术规范、标准和程序，包括开通数字身份所需的凭证类型和验证方法等（例如现场检查护照的可信度就会很高）。另外，增加可存储在客户设备上的生物特征数据也可加强可信度。这些都可以更有力地保证发出请求的人已经获得行动授权。部分国家已经制定了验证标准，如美国国家标准技术研究所（NIST）制定的标准。不同场景下的最低获准分不同：例如，你可能需要更高的评分才能授权批准高价值金融交易。

当前私营部门参与较多的是另一种数字身份：大型科技公司提供的“单点登录服务”（Single sign on service），即“使用……登录”，为消费者提供了方便简化的服务登录方式，使他们能够访问多种在线服务，如电子商务和社交媒体等。然而如果不与现实世界的身份证件相关联（如经政府核实签发的身份凭证），这类数字身份就不能用于对消费者身份可信度要求较高的服务和产品。随着近期美国部分州将驾照纳入移动设备的数字钱包，大型科技公司也开始涉足数字身份验证领域。

更广阔前景——集成数字身份

基础数字身份只是一个开始。利用集成数字身份，用户能够以安全的方式绑定更多个人数据。例如，求职者无需分享任何文件就能向用人单位确认其教育资格或居住状况。同样，病人能够凭借集成数字身份向就诊的医院和医生分享其过敏症和病史信息，这在紧急情况下尤为有用。

数据三角交叉核验提升了信息整体的可信度，从而进一步提高消费者的身份的安全性，这与当前结合实物身份证件和水电记录来核实客户地址的方式类似。强化数字身份需要在身份证可用性和用户体验之间做出权衡。为了从起始阶段就能吸引到一定数量的用户，开通数字身份的流程必须简单。后续为了完善数字身份证，可以增加附加属性，方便用户获取更高级验证需求的产品和服务。

集成数字身份可以呈现为“钱包”形式，允许个人根据具体情况出示特定凭证。这种方式更为强大的应用是让消费者根据数字凭证进行智能决策。例如乘客能够根据其新冠疫苗接种状态或核酸检测结果，以及航班目的地适用的新冠疫情防控措施等，向航空公司确认他们能否安全登机。另外还可以帮助客户在有不同KYC流程要求的银行进行注册，将新银行的KYC要求与原银行客户已核实的身份凭证相匹配。

未来，在开放和嵌入式金融以及更广泛的“开放数据”经济赋能的应用场景中，消费者能够利用集成数字身份自主可控地共享数据。这将为银行客户提供一系列全新的体验：例如在同一点查看所有财务数据、无缝切换至新的能源供应商、实现自动存款转换或提供个性化产品，如基于消费者生活方式的各个方面提供全方位的保险。

1 Vipps International， 2021年4月。

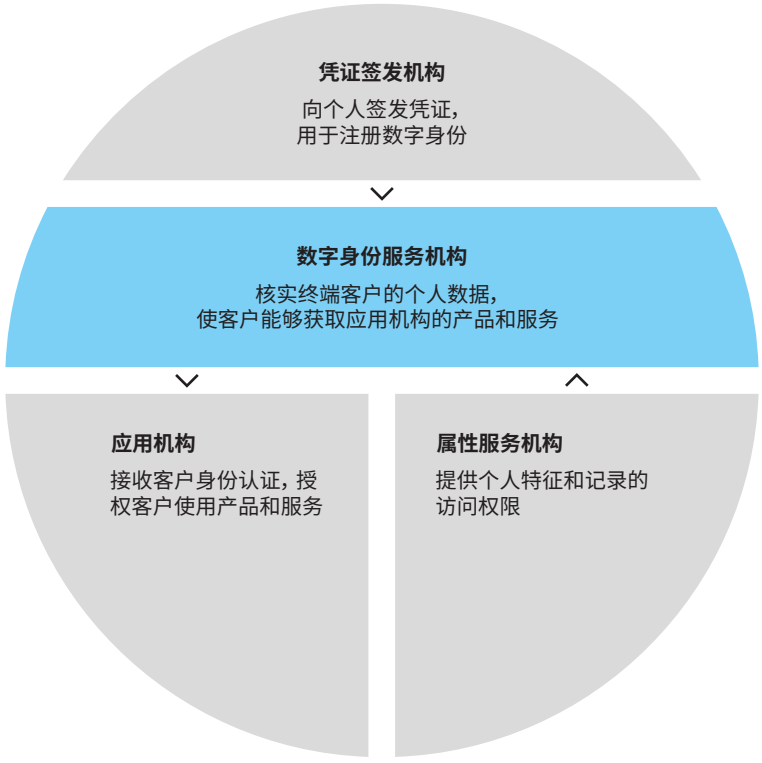
在这类应用中，客户希望且应对数字身份生态系统中各方使用其数据的方式及场景拥有明确的控制权，同时客户只需分享具体用途所需的最少数据。从隐私保护和消费者信任的角度来说，理想做法是身份验证机构（例如银行）除在预防金融犯罪情况下可共享数据外，在其他情况下尽可能仅提供身份确认信息（被称为零知识证明），但不涉及实际数据共享。

数字身份的生态系统

目前仅有少数国家启动了国家层面的数字身份计划。尽管许多计划或生态系统由政府主导，但也有很多是由私营部门发起的。

在所有计划中，数字身份都需要依赖于一家或多家**凭证签发机构**。签发机构签发身份凭证，个人用户才能用它开通数字身份。一直以来，在实体身份证制度中，凭证签发机构通常是政府部门；在数字身份（电子身份证）领域，一些国家也由政府部门负责签发凭证，如爱沙尼亚和中国。在另一些国家，凭证签发机构也可以是银行，个人可通过银行账户开通数字身份，尽管首次开通银行账户往往仍需要使用最初由政府签发的实体身份证。

图 2: 数字身份生态系统中的参与主体



来源：奥纬咨询分析

数字身份服务机构处于数字身份生态系统的核心，发挥着重要作用，负责验证个人身份，使其能够获取数字服务（见图2）。**应用机构**在新客户注册，以及在后续的支付、账户访问和电子签名等验证过程中，都需要使用数字身份服务机构提供的服务。

属性服务机构可验证某一身份属性，并为数字身份服务机构提供访问客户数据记录的权限。例如，加拿大金融服务公司能够按照客户指示，通过“Verified.Me”向应用机构提供数据。信用评分等数据应始终由属性服务机构保管，如用户决定分享，数据则应加密传送，同时由区块链将数据的完整性证明存档。

政府和私营部门主导的数字身份计划

目前出现了两种主要的数字身份生态系统原型。在政府主导的计划中，政府通常是凭证签发机构，除此之外，政府还充当数字身份服务机构。政府可自行实施计划，如爱沙尼亚和新加坡，或者将计划外包给私营部门相关企业，如意大利（见图3）。应用场景最初往往集中在获取政务服务上。

在私营部门主导的模式中，私营部门无论是单独运营还是与其他公司合作，都扮演着数字身份服务机构的角色。私营部门通过KYC程序确立其验证方身份，其中涉及验证政府身份凭证且通常需要匹配官方原始信息。私营部门的数字身份计划可采用公私混合治理的监督模式，如挪威的“BankID”模式，也可采用仅让政府制定指导原则的模式，如加拿大。

中国的数字身份生态体系内有多个数字身份计划，既包括公共部门独立运营的数字身份计划，也有公私部门合作提供的数字身份计划，私营部门提供类似“钱包”这样的运用场景，而公共部门提供身份验证服务。同样，比利时也既有政府签发的电子身份证，又有公私合营的数字身份计划（“itsme”）。电子身份证需要利用实体读卡器进行验证才能获取数字服务，可用于（但非必须）注册“itsme”，“itsme”设有手机应用程序，可供获取包括政务服务在内的多种服务。“itsme”目前是公私合营的数字身份计划，由比利时政府、银行和电信公司共同投资。

图 3: 政府和私营部门主导的全国性数字身份计划

典型案例	政府主导		银行/私营企业主导	
模式	政府发行并运营	政府发行，外包运营	混合治理，私营部门运营	政府指导，私营部门合作运营
治理方	政府	政府	政府或私营部门	政府制定指导原则
计划实施方	政府	私营部门	私营部门	私营部门
责任方	政府	政府或私营部门	私营部门	私营部门
示例	• Singpass（新加坡）	• SPID（意大利）	• BankID（瑞典） • BankID（挪威）	• itsme（比利时） • Verified.Me（加拿大）

政府主导　政府和私营部门主导　私营部门主导

来源：汇编自国际清算银行资料

2. 银行在数字身份计划中的角色

即使在已经推行数字身份计划的国家，也没有一个生态系统能够覆盖数字身份所能提供的全部服务。因此，银行仍有机会发挥主导作用，帮助国家和个人客户从数字身份中获益。

银行想要参与塑造不断演变的数字身份生态系统，就需要明确角色定位。即使银行是作为应用机构有限度地参与，也能够降低成本，减少欺诈行为。另一种参与度更高的方式就是直接参与或者以运营(服务）机构的身份参与计划，这样便能够发掘重要的新盈利点，获得长期的战略收益。

银行的关键作用

银行参与能够确保数字身份计划更可靠、安全和方便。银行被人们信任并受委托管理人们的资金。作为管理人们资金的必要条件，银行可管理人们的个人数据。银行的运营受到强监管，需要遵循严格的反洗钱程序和重要的个人数据保护规定。银行定期管理数字身份数据属性，对个人信息进行适当的尽职调查和保护，并减少数据被犯罪分子滥用的风险。此外，银行已实施可靠的客户开户流程，具有最高安全级别，必要时分支机构还能验证实体凭证。此外，银行的商业模式不需要利用客户的个人数据通过广告或向第三方销售来增加收入。

建立数字身份网络所面临的挑战之一就是必须迅速扩大客户规模以达到足够大量可以影响市场的水平。但早期实施机构往往只能看到局部利益，这使得银行面临的挑战更加严峻。银行在实施安全网络、支付渠道和SWIFT网络等其他支付系统方面有合作和参与的经验。总体而言，银行可能拥有私营部门内最庞大且经过最严格验证的客户群体，因此能够有效地为客户开通数字身份，某些情况下甚至无需重新验证客户身份（至少在开通时无需）。银行服务需要频繁与客户接触，方式也高度安全，很适合成为数字身份计划的首个应用场景。因此，银行在协助塑造数字身份所需生态系统方面处于有利地位，而且必然会与许多不同类型的机构展开合作。

在单一数字身份计划应用程度不高的国家，比如英国、南非或日本，银行显然还有机会协助开发解决方案。欧盟委员会于2021年提出的《电子身份认证与可信服务条例》（eIDAS）修正案要求所有成员国在2022年9月前制定一个框架，提供集成度更高的数字身份，即“数字钱包”框架，这凸显出在欧盟建立数字身份计划的迫切性。欧盟的提议目标宏大，要求成员国开发集成数字身份钱包，用于个人证件存储和属性共享。数字钱包在整个欧洲范围内都将得到认可，而银行则必须作为应用机构接受这一框架。这是首批区域性协调办法之一，在未来一定时间内会为银行提供履行使命、发挥主导作用的机会。

在数字身份应用程度较高的国家，比如新加坡（53%）[2]、比利时（56%）[3]和北欧国家（78%）[4]，尚有许多空间可以进一步丰富数字身份。迄今为止，大多计划只提供基本身份证明，因此对这些国家来说，下一步计划将是开发集成身份证，有可能的话还要建立一个开放式的生态系统。

2 Singpass，2021年10月。

3 Itsme，70%的成年人口，2021年11月。

4 包括BankID瑞典和BankID挪威，2021年10月。

参与方式的选择

具体的银行需要决定自身在不断演变的数字身份生态系统中扮演什么角色。银行现有的选择包括作为应用机构接受数字身份，作为属性服务机构提供数据，或作为数字身份服务机构（可能与其他银行合作）。下文将探讨上述角色及其相关商业案例（见图4）。

图 4: 数字身份计划中各类主体的商业案例

参与度逐渐增加、附加收益和成本逐渐累积

	作为应用机构参与 遵守合规要求（例如爱沙尼亚银行）	作为属性服务机构参与（例如加拿大银行）	作为数字身份服务机构运营（例如北欧BankID）
要求	• 与现有数字身份机构签约，建立使用数字身份服务所必需的基础设施 • 向数字身份服务提供商支付服务费（比部分传统程序更便宜）	• 建立验证/共享客户数据的基础设施 • 就上述服务向数字身份服务机构收费（用数据资产盈利）	• 开发数字身份基础设施，以核实客户身份是否能获取应用机构的产品和服务 • 与属性服务机构和应用机构合作确定基础设施要求 • 决定服务的价格结构
收益（财务和非财）	• 减少包括KYC流程在内的客户引入成本 • 减少欺诈行为	• 向数字身份服务机构收取的费用 • 成为客户旅程的一部分（品牌效益）	• 向应用机构收取费用 • 成为客户旅程中心（感知效益） • 完善服务的机会（战略效益）
成本（一次性和持续性）	• 接受数字身份服务机构流程数字化/标准化的一次性成本 • 向数字身份服务机构付费	• 建立和维护应用程序编程接口 • 清洗留存的客户数据 • 重新验证客户身份以符合数字身份服务机构标准化要求	• 建立和维护数字身份基础设施 • 重新验证/录入客户数字身份 • 向属性服务机构付费

来源：奥纬咨询分析

作为应用机构

应用机构在生态系统中相对被动，需要依赖其他实体、机构和计划提供的数字身份来验证新客户。爱沙尼亚银行就是采用这种方式参与国家数字身份计划，利用爱沙尼亚政府签发的数字身份进行验证。

虽然应用机构在商业上获益有限，但由此可节省后续客户录入和持续认证的运营成本，并减少欺诈事件的发生。

即使应用机构在角色上稍显被动，接受数字身份程序也需要对现有的录入流程（一次性成本）重新进行设计。这样做的好处在于，身份验证形式会更数字化、更精简，因此也更便宜。正如反洗钱金融行动特别工作组（FATF）在《数字身份指南》中所述[5]，使用客户数字身份（非面对面身份验证）甚至可以降低风险，避免账户盗用、网络钓鱼和勒索软件黑客入侵等各种类型的身份盗窃问题。

5 请点击此处查看更多信息。

数字身份可以节省多种成本，包括消除现行反洗钱要求的客户录入产生的摩擦，比如定期刷新客户信息，以及登录、支付授权和电子签名等各种后续流程中产生的冲突；数字身份同时也能减少欺诈风险，节省用于欺诈监测和缓解措施方面的成本。新冠肺炎疫情爆发以来，网络诈骗活动有所增加，这更加凸显了此类应用场景的紧迫性。

由于各家银行在用户体验和安全等领域存在利益冲突，因此所有采用这种模式的银行都必须从内部统一对数字身份的需求和期望值。

作为属性服务机构

银行作为属性服务机构能够增加收入。为此，银行需要投资建立和维护身份计划的安全接口。这样，客户就能授权应用机构访问留存在银行的相关数据及其验证结果，例如证明他们有财务能力租赁某处房产。加拿大银行已通过“Verified.Me”计划向大约35家应用机构提供了上述服务[6]。

提供这种服务时银行会向数字身份服务机构（或应用机构）收费，从而实现创收。属性服务机构还能获得一定品牌效益，例如，如果“Verified.Me”上的银行（或其他金融机构）为客户提供了属性服务，其品牌也会出现在客户旅程中。

作为数字身份服务机构

担任数字身份服务机构是最复杂、最高瞻远瞩的做法。银行想要成为数字身份服务机构，就需要建立和维护一套更复杂的安全应用程序编程接口、客户旅程和个人数据存储解决方案（报告第3节将探讨相关设计选项）。在挪威，银行与政府共同投资，组建公私合资企业，在建立挪威数字身份生态系统中发挥了主导作用。

由于身份保障能够为公司带来商业价值，数字身份服务机构可向应用机构收取费用，就像信用卡支付授权服务一样。随着时间的推移，这些费用的收入可能会很可观。从全球范围来说，消费行业每人每年都有超过500个接触点需要进行安全的身份识别。商业条款变化很快，但当前数字身份服务机构以及正在开发阶段的计划表明，向应用机构的收费大约为简单认证0.01美元/次，简单核查（核查证书）为0.20美元/次，严格核查（例如需对比政府来源查验证书或使用红外/紫外扫描）为5美元/次左右。

因此，每年可从每位客户处获得的潜在收入为40美元（见图5），相当于全球每位客户的平均零售银行收入的6%左右[7]，或者按手机上网人数统计，相当于全球市场总规模超过1500亿美元[8]。

6 截至2021年11月Verified.Me的应用机构。

7 奥纬咨询分析，2019年全球零售银行收入2.2万亿美元（Panorama Financial Institutions and Insights Consulting），覆盖人口38亿。2018年（世界银行）。

8 Statista，《截至2021年1月的全球数字人口》。

图 5: 数字身份服务机构的创收机会（每位客户每年）

识别类型	安全认证	简单身份验证	严格身份验证
近似对应美国国家标准与技术研究所标准	AAL2 (双因素认证)	IAL2 (与实体身份证关联)	IAL3 (目前需要亲自到场查验身份证)
向应用机构收费示例 (按美元计算)	0.01	0.20	5
每人每年总次数	300-500	100-200	1-2
大致收入 (按美元计算)	~5	~25	~10
应用场景			
银行和金融	访问银行账户	大额交易	申请贷款
商业和零售	访问在线商户	购买有年龄限制的物品	购房
政府	-	国家选举	申请旅行证件
员工流程	访问公司内网	-	员工入职
公共设施	访问公共设施账户	创建公共设施账户	-
电信公司	访问电信账户	-	创建电信账户
旅行	机票预订	护照认证	-
卫生保健	疫苗接种状态共享	处方验证	-

来源: 奥纬咨询分析

对于选择成为数字身份服务机构的银行来说，实施、推广和持续创新上的成本将是巨大的，并且还有许多障碍要克服。许多应用场景需要在现实世界做出相应调整，因而进程相对缓慢，如机场护照检查或员工大楼访问权限等。想要成功在一个国家推行上述应用场景，大多数居民需要通过该国现有的身份验证方法，如利用国家身份证或生物识别系统加入数字身份计划，进行数字联网。此外，推行上述应用场景还需要提高应用机构对此计划的应用率，因此可能会出现持续不断的价格谈判。事实上，身份验证很可能演变成日常生活中不可或缺的一部分并受到监管，运营商价格和收入将设有上限，使持续提供服务成为一种义务，类似于当前的ATM网络。

长期相关性

随着数字身份更加集成化，在整体经济中的应用更为广泛，数字身份服务机构将成为客户数字生活的中心。因此，如果银行将自身定位为数字身份服务机构，则需要考虑具有战略意义的关键问题：

银行是否有意成为协助消费者提供每次身份认证互动的可靠机构？

数字身份服务机构能够在客户旅程中发挥桥梁作用，其品牌也将融入更广泛的客户体验，还可在遵循所有适当规则和道德要求的前提下，收集额外的客户数据，用于定制或完善服务。

作为集成数字身份服务机构，银行能够掌握更广泛的战略机会，不仅能够识别客户，还能够定制服务、完善端到端客户旅程等。许多银行以及大型科技公司都致力于为消费者提供产品和服务的整体生态系统。

图 6: 数字身份服务机构的战略收益

来源：奥纬咨询分析

政府在数字身份中的作用

毫无疑问，政府是所有数字身份生态系统的关键组成部分，但并非所有政府都选择了扮演同样的角色。

政府是身份验证中的关键角色，扮演着为本国或本地区居民签发政府提供的身份证件的角色。在一些创新市场，政府已经在扮演数字身份服务机构的角色，有些会为居民提供服务，例如爱沙尼亚和新加坡；还有些是在私营部门的参与下共同完成这项工作，例如意大利和中国。

政府也能够担任属性服务机构的角色，为验证和共享诸如居民身份等重要数据提供安全的访问权限。政府还可作为应用机构，允许居民通过数字身份获取政务服务，从而推动数字身份应用。

各国政府的共同点在于都必须负责制定数字身份的立法和监管框架，以便签发和使用数字身份，并负责指导该框架与现行及未来的监管和标准保持一致，包括反欺诈（包括KYC和反洗钱要求）、数据隐私和更广泛的数字经济等领域。数字身份的很多领域都将受制于国家现有的法律框架和背景。例如，在隐私法规限制更严格的国家，数字身份服务机构需要在数据最小化和分发方面采取更多的措施。

政府是否应该扮演这些角色？又该如何扮演这些角色？这些问题的答案取决于政府具体的政策目标和更广泛的政治和监管环境。相关政策目标包括但不限于：通过改进后的产品和服务推动经济增长、创建新企业、提高数字和金融普惠性（参见第3节），以及降低网络伤害风险，例如通过数字身份核实互联网用户年龄，以起到保护未成年人的作用。某些决策将成为政府的取舍难题，例如开放与隐私、普惠性与增长等。

3. 成功推行数字身份

在技术、监管、消费者信任和竞争等领域，数字身份的环境正在迅速演变。对于有意在塑造数字身份方面发挥主导作用的银行来说，窗口期稍纵即逝。

已经成功运营的数字身份计划的经验展现了很多与银行高度相关的关键成功因素（见图7）。

本地条件显然是影响决策的关键因素，例如需要确定所在国家和地区是否已有既定的政府主导计划或政府签发的电子身份证。银行还需要就预期中的银行之间或银行与其他行业之间的合作程度做出战略选择。在这个过程中，银行业协会将发挥重要作用，协调并促进银行之间以及银行与其他行业在数字身份方面的交流。

为建立和培养公众信任，银行应将推动数字普惠性和遵守商业道德作为工作的核心。消费者对数字身份服务机构和生态系统数据安全性的信任是成功的基础。

业务规模是另一个决定性因素。早期经验表明，在一项私营部门计划中，占据80%市场份额的数字身份合作联盟能够从庞大的用户群体中获得巨大收益。

图 7: 国际银行业联合会成员国的部分经验

详细介绍请参见附件

- 即使没有政府电子身份证，银行也能够推行跨行业计划
- 银行、支付机构和科技公司均能作为数字身份服务机构（与国家合作提供）
- 拥有大量人口的国家能够适应多种采用不同方法，具有竞争关系的计划共存
- 金融机构能够利用数据提供“集成”身份服务，例如无障碍保险应用支付机构正在进入数字身份领域
- 基于合作历史，银行与电信公司合作能够加速计划实施
- 利用各行业的丰富数据解锁一系列服务，但也带来了数据风险
- 大国很难制定单一的总体计划
- 没有良好应用机构应用场景，计划很难推广采用
- 政府电子身份证可实现快速普及应用
- 可在较小用户群体（如政府官员中）试点数字身份计划
- 在政府身份证普及率较低的地方，需要利用生物识别技术（包括语音）开通数字身份
- 从前没有政府身份证的居民能够使用生物识别技术开通数字身份
- 数字身份证普及能够改变投票等公共服务
- 政府能够创建数字身份证计划（利用数字身份证），私营部门作为应用机构
- 私营的数字身份服务机构能够接入政府主导的生态系统
- 政府能够通过政府相关的应用场景和投资来支持私营部门的计划

资料来源：奥纬咨询、国际银行业联合会分析

在下一节中，我们将探讨当今世界各地银行为实现数字身份所做的选择，重点探讨客户价值主张，协作和治理，商业模式和责任，技术、数据和标准，以及商业道德和普惠性等领域。

客户价值主张

数字身份的推行要以目的为导向才能保证后续增长。如果用户能够通过数字身份获取其他服务，其注册的意愿就会更高，所以早期的应用场景需要与消费者的日常生活高度相关或对消费者十分有利。与其从一开始就建立“大而全”的通用型数字身份生态体系，不如集中精力通过“小而精”的明确应用场景打开局面，加快推广应用，形成商业化发展态势。“小而精”的应用场景可以是金融服务，也可以扩展到金融之外，其应用场景的应用还能加强人们对数字身份的认知。频繁使用数字身份的应用场景能凸显数字身份的便利性，同时也能暴露传统身份识别过程的繁琐。积分或折扣等额外奖励也能够推动数字身份的应用，这对于在早期积累必要的用户和客户数量时尤为重要。

在印度，政府签发的电子身份证 “Aadhar”的首个应用场景是为了有效地向农村地区发放福利款。比利时选择使用“itsme”共享新冠疫苗接种状态，使得开通数字身份的人数猛增——现在大家都已习以为常。英国多家银行合作推行的数字身份计划目前专注于开发银行业务的应用场景，一旦证明有效，便可向非金融应用机构提供解决方案。而其他银行则专注于业内和非金融服务应用场景。

新冠疫情已经为数字身份提供了多个新的应用场景。除了用于证明疫苗接种状态外，还可用于证明快递包裹的病毒无接触史。从中期来看，数字身份还可以用于推动央行数字货币的应用。

协作和治理

数字身份计划需要开发涉及多方的网络，因此，协作开发的模式以及政策制定者的支持至关重要。

协作模式能够加速交付，还能分摊研究和开发成本。一些国家和地区在推行数字身份计划时，都会由多家银行共同投资一个商业实体，如加拿大的“Verified.Me”（当前由“SecureKey”管理）、比利时的“itsme”和北欧国家的“BankID”。随后上述商业实体需要确定商业和责任模式、运营模式、技术和数据安全选择，有效地为数字身份生态体系及参投银行建立“信任框架”。为了加快交付速度，银行可能需要与现有网络中的其他成员（如支付机构）密切合作。

在一些国家，只有相对少数银行能够触及全国80%左右的居民，协同开发通常能够取得更好效果。在美国这样拥有数千家银行的市场，在单一银行主导的计划上开展合作显然具有挑战，因此在合作有效推动整合或实现互操作性之前可能会存在多个并行计划。

随着数字身份的发展，基础数字身份的互操作性将变得至关重要，这已经在多种不同的已开展的数字身份计划中体现。互操作性标准能让消费者在不同数字身份体系中及跨越国界使用其数字身份。欧盟和非洲已经致力于开发各自区域内的合作实施计划，这将需要区域内的各市场参与者就共同标准和框架达成一致以提高互操作性，特别是在技术和身份验证评分标准等方面。在欧盟，相关共同标准和框架还需要符合《欧盟支付服务修订法案》第二版（PSD2）、《通用数据保护条例》（GDPR）和《反洗钱指令》（AMLD）等区域性法规。

然而，互操作性的实现充满挑战。不同国家和地区对于有效身份证件类型的要求和认定及各国人民对身份数字化和数据隐私规范等看法存在重大差异，这意味着真正实现数字身份在全球范围内的互操作性可能需要一个漫长的过程。尽管如此，即使各国数字身份生态系统尚处于起步阶段，也应将实现数字身份互操作性全球化作为长期目标。全球安全身份网络（Global Assured Identity）正是致力于实现上述目标的国际组织，该组织定期组织论坛，推动跨国界数字身份的发展。

对大多数的市场而言，围绕数字身份展开的协作或许也将促进KYC程序效率。数字身份能提供可重复使用的身份验证，有助于实现和加快KYC程序。因此已经在KYC程序中开展合作的银行或其他金融机构有机会在现有合作框架下扩大合作范围，推动数字身份计划的建设，促进数字身份生态体系的进一步发展。

跨行业或公共部门的合作能够加快数字身份发展。例如，可引入电信公司和支付机构，这些行业同样处理敏感客户数据，因此也可能需要严格的身份验证。同时，这些行业还拥有维护重要网络基础设施的经验。在中国，支付机构就已经与政府合作开发了数字身份钱包。

除了颁发凭证外，政府的参与也有助于加快数字身份的落实。美国的私营部门近期提出了相关政策建议，呼吁政府部门投资早期私营部门的相关项目。关于应该是由美国政府还是由私营部门来主导美国的数字身份计划的讨论进行，其中如何借数字身份计划实现这一契机推动金融普惠是关键议题。

商业模式和责任

数字身份计划的商业模式，包括如何明确关键价值以及实现价值交换等，将随着数字身份计划的所有权、定价模式和权责分配机制确认后确定。

当前与数字身份相关的大多数定价模式是服务提供机构按身份验证次数向应用机构直接收费，而不是对最终使用用户收费。定价模式通常以阶梯模式进行，以高用量低单价的模式促进销售数量。一些已实施的数字身份计划为了提高在不同合作渠道和服务中的应用率，开始向应用机构按用户数量收费。这一做法根据现有的案例需在单一数字身份计划累积数百万用户后才具备商业可行性。这对于希望自行发展计划的小国家来说具有参考意义。

作为应用机构，银行可通过多种方式利用数字身份实施KYC政策。在最低限度应用中，数字身份能为银行提供在KYC流程和标准所需的部分“预填入”（Pre-population）客户数据。在最大限度应用中，银行能够使用其他银行已经完成的身份验证来开展自己的KYC流程。在不同的数字身份应用场景中，银行面临的欺诈风险都会降低，但不会完全消除。

在基于原则的金融监管国家，银行需要自行制定KYC政策与程序。在这种情况下，KYC流程和标准若要做到全面合规，银行需要对客户身份共同验证标准和评分体系的商议工作投入更多资源，其中可能还涉及立法和 / 或监管。

数字身份的责任模式应明确发生任何错误或后续欺诈行为的情况，并区别服务提供机构在“预填入”与“完整身份识别与验证”服务中的权责差异。对于希望扮演数字身份服务机构或采用相关数字身份服务的应用机构，均须确保了解相关身份识别验证服务和对应任何潜在身份验证识别失败风险。

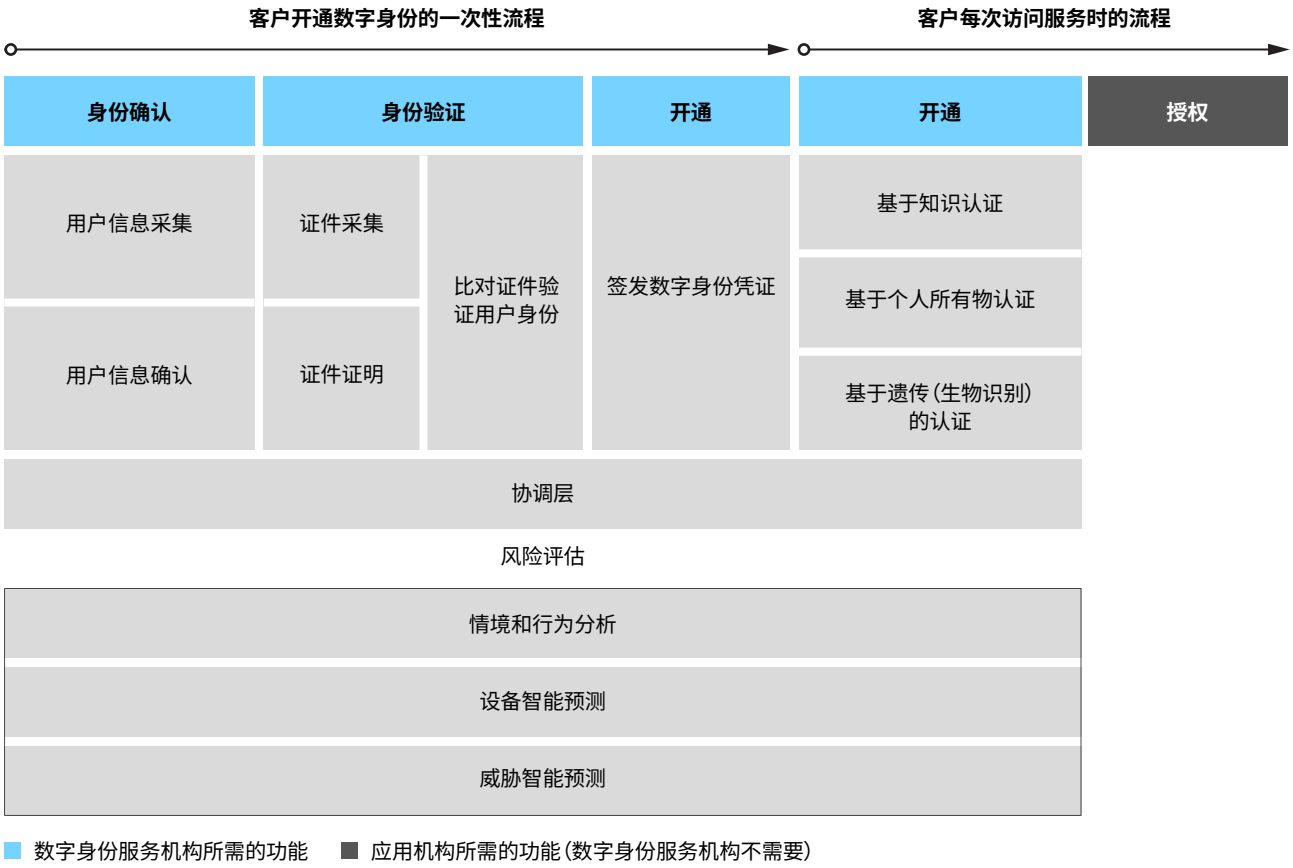
跨境使用数字身份也引发了类似的接受度和责任归属方面的挑战。寻求在别国开展业务的数字身份机构需要遵守当地的数字身份标准，不过由于部分区域标准的统一化，实现这一要求已更为简单（关于欧盟和非洲当前采取相关行动的更多信息，参见前文的“协作与治理”部分）。

技术、数据和标准

最初设计数字身份时，不仅需要考虑技术和数据模型，还需要遵守当地隐私法规（如欧洲的GDPR）、网络安全和身份验证标准（如美国的NIST）。针对银行是否应该重新验证国家 KYC要求和标准实施之前录入的客户这一议题，目前在许多司法管辖区都存在争议。开放身份交换组织（OpenIdentityExchange）等多个领先的全球联盟正在推动制定开放标准和协议，包括万维网联盟（W3C）的去中心化身份识别标识标准，及OpenID Connect（OIDC）认证协议，并有意建立数字身份计划的银行能够应用相关标准，集中精力解决实施问题。当然，技术标准的制定要以现有的数字身份计划为基础。

数字身份开发者同样能够尝试利用现有技术解决方案。目前很多技术供应商至少已经能提供端到端身份验证和认证过程的部分功能。下文将探讨数字身份计划在录入和认证过程中需要的主要功能。

图 8: 客户身份验证、签发和认证所需的功能



来源: Celent

数字身份流程可通过多种不同方式实现，具体实现方式将会影响客户旅程和数据存储。有些数字身份计划主要是录入用户，包括验证用户身份，以及签发数字身份证用于后续认证，发证机构拥有用户的身份数据。还有一些数字身份计划会利用银行等其他机构现有的验证和核实程序，侧重于提供验证身份所需的基础设施，在这种情况下，银行拥有客户的身份数据。集成数字身份可能同时使用上述两种方法，例如虽然是“itsme”直接录入了用户，但其“疫苗护照”服务却由“CovidSafe”负责采集和存储数据。

商业道德与普惠性

数字身份可能会改善金融和数字普惠，也可能适得其反。如果实施得当，数字互动会因此更容易、更安全，居民进行网上活动的信心将增强，也会有更多人加入数字经济。然而，数字身份本身并不能将所有被数字化排除在外的人带入数字领域，银行还需要继续通过其他方式为这类客户提供服务。

银行也能够利用数字身份积极采取措施促进金融普惠，例如利用身份相关的丰富金融数据提高居民的信用评分。印度利用生物识别技术，为从前没有政府身份凭证的居民登记了“Aadhar”数字身份，而“Aadhar”能够用来开设银行账户。在数字身份的帮助下，银行账户保有率在六年内从35%跃升至了80%。美国联邦贸易委员会正在研究向没有银行账户的人群发放数字身份证的可能性，包括被拐卖人口等失去传统身份证明的人。银行应该尝试在全球范围内寻求合作或套用这些举措。此外，确保基础数字身份的全球互操作性对移民群体的福祉也至关重要。

无论银行在生态系统中扮演什么角色，都需要帮助确保数字身份的道德性、安全性和高效性。即使作为应用机构，银行也需要遵守安全和道德守则，保护用户免受欺诈，防止身份数据被非法使用。如果银行成为数字身份服务机构或属性服务机构，共享属性时必须满足客户授权以及数据最小化的要求。个性化应当仅用于为客户提供额外利益，而不是为了银行的利益而影响或利用客户。从技术的角度来看，不管是集中式还是分布式模式，都应该优先考虑如何安全保存数据。对于集成数字身份而言，如果身份相关数据来源不同，例如来自电信公司或雇主等，则应从源头保存数据，防止形成易受黑客攻击的数据“蜜罐”。

结语

为消费者提供和完善数字身份服务是所有国家和地区面临的一项重要挑战，成功推行数字身份不仅需要政策制定者和监管部门采取行动，银行也需要参与进来。既需要个别银行参与，也需要整个银行业共同的努力。

下文将探讨生态系统内各参与者在促进数字身份转变的过程中需要采取的关键措施，这些措施能确保数字身份既能为消费者的日常生活提供巨大价值，又能保证安全，这将加强消费者的信任感，也能降低风险。

单家银行

- 需要高层支持推行数字身份，并确保运营、风险、合规和技术等所有业务人员能广泛理解数字身份的影响
- 做出与其目标匹配的关键决定：做数字身份服务机构还是应用机构
- 建立所需关系和网络；确定技术选择，并进行投资；与KYC流程相结合

整个银行业

- 在银行之间、银行与其他行业以及银行与政府之间开展商谈，确定能为客户提供最佳数字身份计划的模式：政府发行并运营还是政府和私营部门联合运营等
- 银行之间或银行与其他行业需要合作制定共同标准
- 支持和提高不同计划之间和国家之间的数字身份互操作性

银行业协会

- 为会员单位组织论坛，提供专业知识，促进对话交流和集体行动
- 协助制定进度和目标，制定实施和推广数字身份的进度要求
- 促成与相关政府部门的沟通，参与制定相关政策和立法，确保消费者受益

政策制定者

- 协助和扶持新数字身份服务机构，必要时进行投资支持，分享其他市场的经验，邀请私营部门参与决策，促进新数字身份生态系统的加速发展
- 确保开通数字身份证属自愿行为，立法需规定关键服务必须提供非数字化的访问方式，防止部分人民被排斥在服务外的情况
- 支持鼓励投资数字身份证服务机构的生态系统，例如通过拨款、税收优惠、补贴、监管等方式(见下文）

金融服务和数据隐私监管机构

- 与政策制定者合作，确保国家数字身份与数据隐私、反洗钱和 KYC、网络安全、责任和数字身份等方面的政策和法规相匹配
- 设定数字和非数字世界提供金融服务的预期
- 建立一个明确的、基于原则的监管体系，该体系根据参与者对该体系造成的风险相匹配，允许新进入者参与并有机会发展壮大

附件-各国和市场的数字身份概况

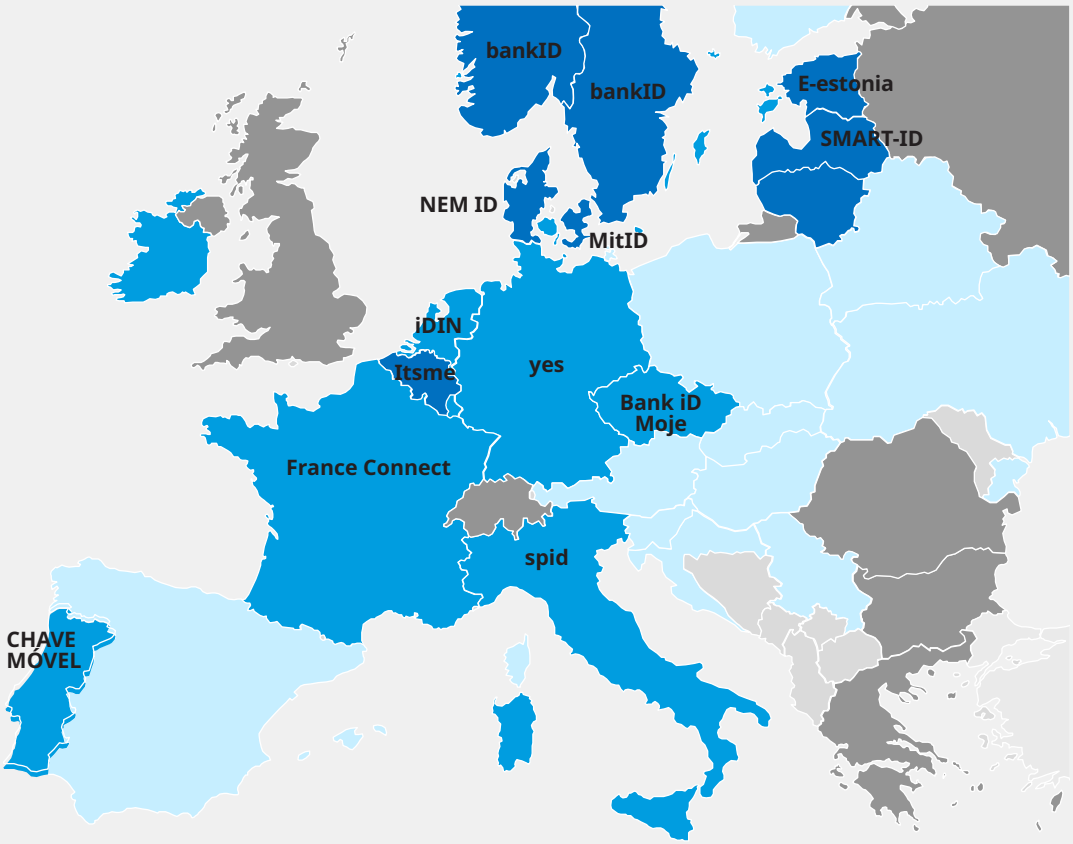
欧盟：各国协作，将数字身份引入欧洲

拟议数字身份钱包

- 《电子身份认证与可信服务条例》的一项新修订案要求所有欧盟成员国制定数字身份计划
  - 由公共或私人部门提供
  - 国家及部分私营部门（如银行）有义务接受数字身份计划
  - 必须遵守符合公民利益的原则，包括数据最小化和公民控制（针对存储和共享的数据）

  欧盟将召开公共部门-私营部门联合论坛，商定统一的操作和技术标准，旨在推动跨欧盟数字身份互认
- 要在欧盟范围内达到应用率80%的目标，尚有很多工作要做：
  - 目前只有少数成员国拥有成熟计划
  - 诸如SPID等其他计划现阶段仅可用于政府服务

欧洲当前的数字身份状况



1. 成熟的计划，是指应用率超过40%。; 2. 现行的计划/电子身份证，是指应用率超过5%。
来源：专家访谈、欧盟出版物、欧盟电子身份证用户社区

北欧：首个银行主导的数字身份计划

银行能够建立适用于所有人的计划，21世纪初建立时还没有政府电子身份证，现在BankID已经有超过5000个应用机构。

概述	主要特点
数字身份计划 • 主要特点 **国家模式** 混合治理，与私营部门合作 **综合应用率** 78% **获取方式** 手机应用程序 **是否使用电子签名** 是 **可共享属性** 核心身份数据 **应用机构数量** 约5000家	**客户定位** • 向客户签发BankID，通过银行进行真实性验证 • 可用于贷款申请等金融服务，纳税申报等政务服务、医疗服务 • BankID可适用于KYC程序，但无法取代KYC程序，银行正在发展独立的KYC专业机构 **治理和协作** • 瑞典和挪威的主要银行就各自的BankID开展合作 • 与其他应用机构所在行业展开合作，但迄今为止在附加属性方面的合作有限 • 为了改良其产品，2014年挪威Bank ID与金融科技公司Vipps和BankAxept合并 **商业模式** • 银行作为主要的初始投资者，建立独立商业实体 • 根据验证次数向应用机构收费 **技术和数据模型** • 识别客户数据，由BankID计划集中留存，从而共享交易监控工具

中国：相互竞争的计划有助于推动应用和创新

人口众多的国家能够通过采取不同的方法来适应多种存在竞争关系的计划。银行、支付机构和科技公司都能够与政府合作推行计划。

概述	主要特点
数字身份计划（示例） • 政府电子身份证 • 政府颁发的“互联网+”可信身份认证，由中盾安信提供支持 • 国家服务平台 • 中国工商银行 • 支付宝 • 腾讯/腾讯云 **国家模式** 政府签发，政府/国有机构验证，（主要由）私营部门提供 **综合采用率** 60-75% **获取方式** 手机应用程序、应用程序编程接口、银行卡 **是否使用电子签名** 是 **可共享属性** 政府持有数据（包括医疗数据） **应用机构数量** 私营部门比例高	**客户定位** • 大多数银行、支付机构、科技公司和政府部门都有独立的交付渠道或政府电子身份证“钱包” • 可远程和面对面用数字身份获取政府、金融服务、娱乐、旅游和其他服务 • 目前安全性低于实物身份证件，例如不能用于开立具有最高安全级别的银行账户 **治理和协作** • 在提供身份服务方面，政府负责对比记录核验身份，私营部门则负责推行计划 • 政府资助数字身份证技术的研究和开发，促进各计划之间的兼容和识别，提高其通用性 **商业模式** • 大多数计划按验证次数向应用机构收费，有些技术公司也会按验证算法或模型收费 • 大型科技公司根据生物识别（面部）数据而非政府持有数据验证用户，收费较低，适合安全性较低的应用场景 **技术和数据模型** • 政府存储核心身份数据 • 更多集成数据存储于使用区块链技术的分布式结构中，包括新冠疫情健康状况和教育史等

加拿大：基于区块链的集成身份计划

整个金融业可以跨服务项目通力合作，创建集成身份计划，提供信用核查和无障碍保险申请等服务。支付服务机构也在向数字身份市场进军。

概述	主要特点 旨在满足并超越KYC/反洗钱合规要求下的数字客户录入准则
数字身份计划 • Verified.Me **国家模式** 政府指导，私人部门提供 **应用率** 30-50% **获取方式** 手机应用程序、网络 **是否使用电子签名** 是 **可共享属性** 身份和金融服务数据 **应用机构数量** 45家 **渠道** 面对面、移动网络、互联网、呼叫中心、从纸质到数字	**客户定位** • 应用于金融业和政府部门，并开始进入商业和健康保险、法律、房地产等其他领域 • 可共享金融合作机构提供的“集成”金融数据（银行、财富、保险） • 多数据源：政府、电信公司、银行、征信机构 **治理和协作** • 7家主要金融机构合作 **商业模式** • Verified.Me作为在整体经济中运营的市场服务，现已获得支付机构Interac授权 **技术和数据模型** • 分布式模型，身份服务机构和属性服务机构持有数据（用户设备上有数据指针），然后与应用机构进行安全合作，利用区块链提供完整性证明 • SecureKey提供技术 • 基于已成功推行的政府登录服务（2012年投入使用），已有1800万加拿大人安装

爱沙尼亚：政府推行的数字计划

普及电子身份证能够转变包括投票在内的各种公共服务，支持政府（智能身份证）计划，私营部门已作为应用机构成功加入计划。

概述	主要特点
字身份计划 • E-estonia **国家模式** 政府签发和实施 **应用率** 电子身份证99% 智能身份证44% 移动身份证19% **获取方式** 芯片卡，手机应用程序，SIM卡 **是否使用电子签名** 是 **可共享属性** 核心身份数据 **应用机构数量** 约200家（智能身份证）	**客户定位** • 通过政府提供的“智能身份证”可获取政府服务、公共设施、金融服务、教育、商业、医疗保健和其他方面服务 • 实现了政府服务的广泛数字化应用 **治理和协作** • 由政府提供，私营部门公司接受认可 **商业模式** • 智能身份证明服务机构按交易次数向应用机构收费，并实行分级定价 **技术和数据模型** • 居民根据实际情况，可选择通过芯片卡读取电子身份，通过手机应用读取智能身份证，或通过SIM卡读取移动身份证

比利时：跨领域合作

银行与电信公司的合作历史证明合作能够加速计划实施。政府部门实施认证应用场景能够促进发展(但须确保计划符合《电子身份认证与可信服务条例》规定）。

概述	主要特点
数字身份计划 • Itsme **国家模式** 私营部门提供，政府主导监管框架 **应用率** 70%的成年人口（占总人口的56%） **获取方式** 手机应用程序 **是否使用电子签名** 是 **可共享属性** 核心身份数据，待添加其他属性 **应用机构数量** 约400家（公共部门和私营部门）	**客户定位** • 所有持有政府电子身份证的居民均可注册itsme • itsme提供身份识别、认证、交易确认和数字签名等服务，还可实现跨领域获取服务 • 2018年，itsme可访问公共服务时，以及2021年6月被用作比利时Covidsafebe应用程序的认证办法时，应用率飙升 **治理和协作** • 由7家银行和电信公司合作推出该计划，政府最近作为投资者加入 • 欧盟《电子身份认证与可信服务条例》认定该计划的身份识别认证为“高”级别，可信服务/签名认证为“合格”级别 **商业模式** • 服务按用户人数定价（不考虑交易数量） • 电子签名按交易次数定价 **技术和数据模型** • 核心身份数据采用中央数据存储模式（所有数据都经过严格加密） • 其他数据属性采用分布式存储模式（为避免数据重复，数据仍存储在真实源中），itsme不可查看交换的数据

印度：跨部门共享集成数据

通过使用生物识别技术注册，Aadhaar为许多印度公民首次提供了一个官方身份。来自经济各领域的集成数据催生了一系列服务，但也引发了人们对数据隐私问题的担忧。

概述	主要特点
数字身份计划 • AADHAAR **国家模式** 政府签发和实施 **应用率** 91% **获取方式** 身份证号码 **是否使用电子签名** 是 **可共享属性** 不同行业内的多种属性 **应用机构数量** >3500家	**客户定位** • 通过与服务机构共享Aadhar号码（或“虚拟”生成的号码）的方式运作 • 首个应用场景是新冠肺炎疫情期间备受关注的社会福利发放 • 目前适用于多种服务，包括开设银行和电信账户、通过谷歌Tez平台付款等 **治理和协作** • 由政府发起和管理 • 目前私营部门正使用应用程序编程接口在Aadhar的基础上创建服务，例如支付服务 **商业模式** • 自2019年起向应用机构收费：每次认证费用为0.007美元，每次电子版KYC交易费用为0.3美元 **技术和数据模型** • 使用生物识别技术向居民签发Aadhar号码 • 与具体应用场景相关的分布式信息数据库，例如养老金、银行等应用场景 • 2017年因技术错误造成重大养老金数据泄露事故（随后已得到解决）

澳大利亚：政府发起的生态系统

政府计划通常从公共部门的应用场景开始。政府主导的生态系统能够接入私营的数字身份服务机构。

概述	主要特点
数字身份计划 • 澳大利亚政府数字身份 **国家模式** 新兴生态系统 **应用率** 5%-10% **获取方式** 手机应用程序 **是否使用电子签名** 否 **可共享属性** 核心身份数据 **应用机构数量** 目前仅限联邦政府	**客户定位** • 政府计划最初只适用于联邦政府服务，政府正在制定立法将计划扩大到州和私营的应用机构，同时以中小企业为重点 • 获得信任框架认可的少数公共部门和私营的数字身份服务提供商 • 银行、支付和电信行业正在考虑推行私营部门计划 **治理和协作** • 政府启动和管理生态系统，但私营部门可在生态系统内担任数字身份服务机构 **商业模式** • 待私营部门加入生态系统后方可确定 **技术和数据模型** • 目标状态是在多家身份服务机构、属性服务机构和应用机构之间的界面创建“身份交换”层

韩国：政府领导技术革新

可在少数用户群中试点实行数字身份计划，例如政府官员。
政府可通过资助新计划鼓励发展区块链技术。

概述	主要特点
数字身份计划 • 政府主导 **国家模式** 政府发布，私营部门提供 **应用率** 不适用 **获取方式** 手机应用程序 **是否使用电子签名** 否 **可共享属性** 核心身份数据、新冠疫情数据 **应用机构数量** 有限	**客户定位** • 政府计划目前仅政府官员可用，适用于公共部门和新冠疫情相关应用场景 • 正在开发更多私营部门计划 **治理和协作** • 政府计划外包给科技公司实施 • 科技公司、电信公司和银行之间广泛的私营部门合作 **商业模式** • 待计划拓展后方可确定 **技术和数据模型** • 在计划中使用区块链技术

美国：技术可用，但无重大计划

大国不太可能推行单一的总体计划，数字身份计划与政府的关系可能会有所不同：在美国，私营部门呼吁政府投资，但由私营部门自行推行计划。

概述	主要特点
数字身份计划 • LOGIN.GOV **国家模式** 政府指导，政府和私营部门新兴计划 **应用率** <5% **获取方式** 手机应用程序 **是否使用电子签名** 是 **可共享属性** 核心身份数据 **应用机构数量** 仅限于公共部门	**客户定位** • Login. gov计划应用场景为获取政府服务，政府进一步投资将其转化成更综合化的数字身份 • 数字驾照（在某些颁发驾照的州）可作为数字钱包凭证，用于旅行等各种用途 **治理和协作** • 政府投资4个“零知识”政府计划 • 银行正在考虑开发数字身份，但由于银行数量超过5000家，因此不太可能仅围绕单个国家计划展开合作 • 市场上有多个小型计划和单点解决方案 **商业模式** • 情况仍在不断发展变化，模式多样且待定 **技术和数据模型** • 市场上有单点解决方案和端到端解决方案 • 分布式（区块链）和中央存储模式等多种实施方式

南非：计划正在开发中

在数字身份计划发展的早期阶段，私营和公共部门可能会展开广泛合作。与印度一样，政府身份证普及率有限的情况下，生物识别技术可能是最合适的注册方式。早期应用场景的合理应用明显需要针对具体的国家情况来定。

概述	主要特点
数字身份计划 • Secure Citizen **国家模式** 政府指导，新兴私人部门合作 **应用率** <1% **获取方式** 手机应用程序 **是否使用电子签名** 否 **可共享属性** 政府持有数据 **应用机构数量** 约10家	**客户定位** • 早期数字身份公司Secure Citizen由OneVault Africa（私营）与南部非洲反防欺诈服务机构合作推出，专注于减少欺诈行为和提升数字普惠性 • 未来计划将触及更广泛的应用场景，但尚未到位 **治理和协作** • 包括Bankserv在内的各行业协会试图号召私营部门和政府部门共同开发数字身份生态系统 • ID4Africa和Smart Africa等机构正在计划在整个非洲地区提供具有共同信任框架的数字身份 **商业模式** • Secure Citizen直接向消费者提供免费服务 • Secure Citizen向应用机构提供两种定价模式： • 对于小批量服务进行分级定价，按验证次数收费（例如信贷申请） • 对于大批量服务（如付款），每月按客户数量收费（不限制验证次数） **技术和数据模型** • Secure Citizen使用多模式生物识别技术（面部、语音和指纹），与政府记录交叉比对，可通过应用程序编程接口或渐进式 Web 应用使用，并适用于聊天商务场景 • Secure Citizen利用协调层，在现有生态系统（数字转型程度不同）之间打造的互操作性

英国：早期计划应用率有限，自2019年以来重新兴起

早期计划的客户和应用机构应用率较低，从2019年起，政府（数字、文化、媒体和体育部）制定的数字身份战略和信任框架重新推动了生态系统的发展。

概述	主要特点
数字身份计划 • POSTOFFICE EasyID **国家模式** 政府指导，新兴私营部门合作 **应用率** <5% **获取方式** 手机应用程序 **是否使用电子签名** 是 **可共享属性** 核心身份数据 **应用机构数量** 有限	**客户定位** • 部分早期计划只提供有限的服务 • 未来计划将囊括更广泛的公共部门和私营部门应用场景 **治理和协作** • 自2019年以来，数字、文化、媒体和体育部主导开发信任框架，支持英国数字身份生态系统，预计将于2022/23年立法生效 • 英国金融业协会和英国投资与储蓄协会等行业协会目前正在召集金融机构，共同商讨各家机构在未来生态系统中发挥的作用 **商业模式及技术和数据模式** • 由于生态系统刚刚建立，尚无具体数据可用

日本：电子身份证是数字身份计划的基础

政府的电子身份证有望迅速普及。

概述	主要特点
数字身份计划 • 个人编号卡 **国家模式** 新兴生态系统 **应用率** 38% **获取方式** 电子身份证卡 **是否使用电子签名** 否 **可共享属性** 核心身份数据 **应用机构数量** 不适用	**客户定位** • 政府近期发行了电子身份证，并计划提供智能手机版本 • 市面上尚无数字身份计划 **治理和协作** • 在数字身份计划概念验证方面，银行与支付机构的合作才刚起步 **商业模式及技术和数据模式** • 由于生态系统刚建立不久，尚无具体数据可用

术语词汇表

属性服务机构 (Attribute service provider) — 指所有允许访问和记录个人属性并将其关联到个人数字身份的机构。根据机构所提供数据的类型和数量，可确定身份属于基础型还是集成型。

认证 (Authentication) — 指使用生物识别技术或密码检查某人是否与某账户，特别是与数字身份相关的过程。

凭证 (Credential) — 为验证个人身份（即“我是我所声称的人”）或与之相关的某些特定属性（如“我有大学学位”）而签发的证件或令牌（实物或数字）。凭证可用于建立数字身份或为身份添加额外的集成属性。数字身份服务机构可自行签发凭证。

凭证签发机构 (Credential issuer) — 指向个人（或其他实体）签发凭证的机构，例如对教育证书而言，凭证签发机构可以是政府或大学。

数字身份 (Digital identity) — 指一种允许用户以数字方式验证或分享个人数据的服务。基础型数字身份包括如姓名、出生日期和居住地址等可识别数据。集成型数字身份包括与个人相关的更广泛的数据集。

电子身份证 (e-ID) — 指以数字方式签发的可授予访问许可的凭证（通常由政府签发）。

身份评分（保证等级）(Identity score (assurance level)) — 当关联数字身份时，它代表验证的可信程度。可通过如下方式提高评分：根据（更多）凭证，特别是政府颁发的凭证验证身份，使用更可靠的方法证明凭证，以及根据不同的数据来源对信息进行三角交叉分析等。不同应用场景会设置不同的最低分数要求。现有多种国际公认标准，例如美国国家标准与技术研究所标准 800 63 3 IAL；GPG 44和45。

数字身份服务机构 (Digital identity service provider) — 指能够验证最终用户使其能够获取应用机构提供的服务和产品的服务机构。

互操作性 (Interoperability) — 指不同数字身份计划之间任何需要互认和进行技术连接的关系。互操作性可实现居民身份通用，例如在不同国家之间通用。互操作性可在用户体验层或技术标准层实现，即用户可以在没有完全实现技术标准互操作性的情况下，体验互操作生态系统。

开放数据 (Open data) — 指一种向消费者开放所留存的消费者数据的广义概念，允许消费者在获取新服务和产品时控制数据访问权限和使用（如开放银行）。

应用机构 (Relying party) — 指所有需要核实和/或验证客户身份才能访问其产品和服务的机构。

验证源 (Source of verification) — 指在验证身份凭证或特定属性时，被视为具有权威性的实体或数据库，通常由该身份凭证签发机构持有。

信任框架 (Trust framework) — 指经各机构同意签署的一系列数字身份计划规则和技术规范。

身份验证 (Identity verification) — 指验证身份凭证以及核查身份持有人是否与所用身份凭证相匹配的过程。

零知识证明 (Zero-knowledge proof) — 指一种直接与应用机构共享验证结论，同时并不共享其具体个人数据属性的验证过程（例如确认某人超过18岁，但并不共享其具体出生日期）。

奥纬咨询是一家国际领先的管理咨询公司，结合了深厚的行业知识和丰富的专业专长，提供战略规划、运营、风险管理及组织架构改造等课题广泛的咨询服务。

如欲了解更多信息，请拨打下列电话联络奥纬相关地区办公室市场营销部门。

中国	亚太地区	欧洲、中东和非洲	美洲
+86 21 6103 5488	+65 6510 9700	+44 20 7333 8333	+1 212 541 8100

中国区业务联络人

钱行
董事合伙人
Hang.Qian@oliverwyman.com

许维珂
项目经理
Weike.Xu@oliverwyman.com