Deloitte.

完美构想

数字身份蓝图

目录

前言 3

数字身份及金融机构角色 4

全球身份挑战 6

数字身份简介 7

数字身份系统概况 8

指导原则 9

好处 10

未来应用 12

结论 13

联系方式 14

前言

尊敬的各位同事：

各行业都根植于突破性技术。冷冻浓缩技术使橙汁成为遍布全球的商品、晶体管是当今电子工业的基石，而麻醉学（以及疾病细菌学理论）则引领了现代外科学的发展。

除此之外，还有数字身份。

目前我们所拥有的身份系统减缓了金融科技创新的步伐并阻碍了金融服务的网络化发展。近在咫尺的全球数字交易只有在数字身份实现的情况下才会发生。

在此背景下，德勤企业管理咨询公司（德勤）及世界经济论坛于近日完成了为期一年的数字身份研究报告《金融服务的颠覆性创新：数字身份蓝图》。研究的目的是什么？目的是了解金融机构在制定数字身份全球标准中应担任的角色。

本文为研究结果的摘要。开篇介绍了身份审查及其对金融科技、金融服务和社会的重要性。之后介绍了数字身份 — 什么是数字身份、数字身份系统是什么、数字身份系统建立的指导原则是怎样的及我们预期可能存在的好处。最后，我们设想了将数字身份应用于金融服务业的若干方式。

如果您关注金融行业未来的发展动向，这份摘要将对您有所助益。这份摘要会帮助您全面了解身份的本质及其在我们生活中更为广泛的应用。我们希望，本摘要会使您体会到为金融机构建立数字身份系统的紧迫性。在阅读完本文后，您可能会认同，现在是时候建立数字身份系统了。

此致

Bob Contri
金融服务全球领导人
德勤有限公司
bcontri@deloitte.com

Rob Galaski
金融服务行业未来论坛 德勤领导人
德勤加拿大
rgalaski@deloitte.ca

数字身份及金融机构的角色

用户身份识别对于金融科技而言是一个棘手问题。如今，需要身份识别的交易，不论是支付、贷款还是其他，都需要通过电子渠道收集实物证据（如对驾驶执照拍照）或依赖金融机构已建立的了解客户（KYC）流程。纯数字金融科技产品亟待开发以解决该问题。

网上交易的关键

作为金融服务流程的核心，客户身份识别十分重要。金融机构需要识别客户身份以确保合规、评估保险和信贷业务风险，以及提供定制化的客户体验。详实及准确是身份识别的关键。数字身份将完善身份识别，同时取消当前流程中主要通过人工完成的环节以提升效率。

但数字身份并非仅与金融服务相关，例如需要身份证明的公共服务，包括养老保障、失业保险、教育、医疗、投票等。私营商业在很多情况下同样需要身份证明，如买酒、租赁公寓及买车等。这使得人们及机构面临身份识别的相关风险。在实体身份系统中，盗用及伪造情况时有发生。

此外，对数字解决方案的需求正日益紧迫。交易量与日俱增且交易愈发复杂。客户希望得到无缝衔接的全渠道服务，如果得不到这种服务，他们宁愿选择在其他地方处理业务。监管方面希望进一步了解交易情况，如果存在身份信息丢失或有误，他们会要求企业承担责任。

最后，数字攻击愈发老练。黑客们比以前更容易入侵脆弱的身份系统，眨眼间便会造成财务及声誉损失。

多层面问题

那么我们该如何看待数字身份系统？一种理解方式是视其为一个多层面的问题。底层为系统运行标准，此类标准需要被制定。顶层则是向用户提供高效、无缝的服务。位于两者中间的问题是授权、属性交换、身份认证及属性收集。各层面的问题都面临着各自的挑战。

目前许多成果都只能解决一个层面的问题。例如，身份认证技术解决方案倾向于依赖已经收集的身份属性。这些解决方案为用户提供更好的体验并确保每次进行交易的是同一个人，但这无法帮助识别这个人究竟是怎样的。

其他解决方案也仅能解决一个特定交易类型的问题。例如，有些解决方案可能有助于政府服务，但也仅限于此。该方法以收集「墓碑」数据（类似人名及死亡日期等）告终，而非收集用以详细描述用户的数据。

最后，我们看到就身份系统建立的标准及流程所达成的诸多共识，往往是以放弃建立一个可用于更广泛商务用途的、成熟的身份解决方案为代价的。

身份层面	目的	问题
服务	向用户提供无缝服务	低效或与需求不符
授权	根据用户属性向有权享有服务的用户提供服务	授权规则及关系复杂
属性交换	提供各方之间属性交换的方法	缺乏安全性和对隐私的保护
身份认证	提供将用户与属性相匹配的方法	认证较差或不方便
属性收集	采集并存储用户属性	属性收集有误或不充分
标准	制定系统运行的标准	缺乏协调及一致性

寻找共同点

这些差异是由于对数字身份的多元化诉求造成的。技术公司、专业组织及政府都在各自开疆拓土，这本身没什么不好。一个有价值的解决方案不一定非要解决全部的问题。

但我们需要将各种解决方案整合在一起，使它们形成一个强大的身份系统。这个身份系统应足够方便、有效，能让用户管理个人信息并在用户使用系统时对用户信息进行保护。这个身份系统应可以处理较大的交易量，且对参与交易的每个人有价值。当然，这实现起来并不容易。

由于金融机构更容易完成数字身份识别，应该由金融机构牵头推动数字身份系统的建立。

首先，金融机构在日常经营过程中经常用到数字身份，包括存储及认证用户信息，且所涉及的业务范围横跨多个司法权区。他们有能力创建新的数字身份系统及标准（参阅：Interac）。在发达经济体，他们的人员、法律实体及资产的覆盖情况已近完善。

此外，金融机构相对成熟。金融机构在对用户数据的操作与使用上受到严格监管。他们在众多交易中担任中介的角色。相比于其他托管机构，客户更倾向于由金融机构来管理自己的信息和资产。

身先士卒的好处

金融机构能从中获得什么？三样东西：效率（及其规避的成本）、收入及变革。让我们来分别了解一下。

效率。可靠、稳固的用户属性库可节约业务过程中耗费的时间并避免可能的人为错误，还有助于创造新的客户服务模式并作出更好的风险预测。

收入。首先，由于更多的客户信息可以更好地反映客户对新产品及服务的需求，金融公司能够以此发掘客户需求获取更大收益。其次，金融机构可与需要了解客户，但是没有或不想保留客户信息的企业合作以获取收益。最后，金融机构还可为虽不购买金融机构产品，但须认证身份的非金融机构客户认证身份以获得收入。

变革。利用数字身份，金融机构可突破其现有业务，可作为其他行业间可信赖的中间人，可为公共部门提供身份服务（例如社会服务及纳税申报）。金融机构还可以要求客户对其个人信息的准确性负责，从而不再需要使用第三方数据挖掘评估客户信用历史。综上，金融机构的服务还可延伸至非金融咨询的服务。

建立身份系统的方法有多种。具体采用哪种方法由具体情况决定。稍后我们将对此进行讨论，但首先，让我们来看一下身份识别给金融机构带来的各种问题。

全球身份挑战

金融机构非常了解收集验证身份信息的困难。合规、尽职调查、了解您的客户 (KYC) ，上述方式都效率不高，尤其是在保护个人信息方面。

这只是比较普遍的问题，还有个性化的问题。且不提服务中小企业的银行所遭遇的挑战，就以零售银行为例，由于缺乏对新客户历史财务情况的了解，使零售银行难以规避客户欺诈和向客户提供适当的产品及服务。

企业和投资银行在身份认证方面也有自己的难题。其中之一是追踪资产源头和所有权。另一个则是监控及追踪资产再抵押。

事实上金融机构所遭遇问题的症结是相同的，均源于仅为支持面对面交易而设计的系统。换言之：我们现代化的数字经济依旧依赖实物记录来认证身份。

那么我们有什么其他的选择呢？数字身份系统又是怎样的？

在数字身份系统中，「身份」是代表用户的一组数字记录。这些记录由提供完成交易所需身份信息或担保的实体依据标准格式存留。数字身份还可以接受并整合新信息，从而实现对用户更全面的了解。

数字身份系统更便于信息资料的采集和分享。此外凭借尖端的的身份甄别技术及安全协议，数字身份系统使得身份记录更难被损毁、丢失、盗窃或篡改。最后，数字身份也为金融服务机构及众多其他客户服务型机构提供了一种更好的了解和服务客户的渠道。

多种前景可观的技术使我们更接近数字身份系统的实现。数据存储技术的进步优化了数字身份系统的用户信息储存能力，同时也使系统能更好的保护用户私隐、安全性更高、用户可控性更强。新数据传输协议在加强防护数据拦截和解密的同时，将更多的控制权转交给用户。新的身份认证技术也在不断发展。这些技术将用户与他们的数字活动以更为稳健、持续的方式联系在一起。

数字身份识别之路并不平坦。虽然全球新技术风起云涌，但有些已然失败。人们不会使用设计不好、运行不流畅或不可靠的系统。除此之外，技术开发难免面临资金不足的问题。系统也可能会存在一些缺陷，例如服务群体太过狭隘或最终与公共政策相冲突。我们在此强调，数字身份必须为人类、企业及社会带来多种利益这一理念。

数字身份简介

身份由多个不同的信息碎片组成，这些信息碎片也称之为属性。属性越多，身份越强。即使某一属性具有唯一性这一理论也是适用的。

例如，国家可向个人发出独一无二的身份编号。但编号本身几乎不会告诉你任何东西。如果你知道此人的姓名及出生年月，就了解得多一点。再加上照片、手机号码、住宅地址、学历档案和工作经历，那么你了解得就更多了。

不仅只有人拥有身份，法人实体（例如公司和信托）和资产（所有权）也拥有身份。你的身份中的属性帮助他人决定是否和你交易——接受你的投票、开立储蓄账户、向你销售酒类等。法人实体和资产也是如此。他们的身份或当中的部分属性，帮助他人决定是否与合适的所有人、代表或托管人开展业务。

身份保证是身份交易的关键因素，指身份属实且属于使用者的可信度。对于网络注册或支付停车费这一类交易可以不鉴别身份是否具有高可信度。但对使用在线经纪账户或获取政府服务这一类交易，则必须保证身份高可信度。这些交易为高保证交易。

另一方面，身份交易倾向依据身份类型形成各种网络。例如，政府身份系统和雇员管理系统均围绕个人形成。商业登记和行业识别系统则围绕法人实体而形成。资产登记则围绕……你们明白的。

但所有身份系统都有一些共同点。他们都有**用户**——在系统内拥有身份，从而可以进行交易的人士。他们还都有**身份提供者**——即储存用户属性、确保信息属实和代用户完成交易的人士。还有**依赖方**，即在身份提供者为用户提供担保后服务用户的人士。

另外，所有系统都有一个管理主体，监督系统运行并制定规则。在此之下是各种平台，通过满足各方所需来完成交易。

到目前为止所述的一切我们并不陌生。历史上人们一直在使用类似的系统。当一个人携带介绍信前往招聘办事处，他就是一个用户。介绍信来自愿意担保用户值得被聘任的人士，推选用户的人士就是身份提供者。介绍信提交的对象就是依赖方。依赖方根据自身的判断和他们对身份提供者的了解决定是否接受介绍信的请求。

数字身份系统也是遵循这一流程，只不过是电子化的，所有事情都是在线上完成。但数字身份有不少的优势。它更便于在交易各方之间的信息共享，比实物文件能容纳更多的信息，再辅之以适当的技术，使用户能更好地控制个人信息如何被储存和使用。

数字身份系统概况

数字身份系统分为五个基本类别。

第一类是**内部身份管理**。在这类系统中，一方同时是身份提供者和依赖方。例如，公司可根据员工的不同属性控制员工对不同服务的使用权限。

第二类是**外部认证**。这一类与第一类相似，但另有一组身份提供者鉴定用户身份。其优势是用户可凭借一组凭证而不是设置不同的用户名和密码来使用不同的服务。

集中身份是另外一类。在这类系统中，一方（例如政府）作为将用户属性传送给各依赖方的身份提供者。例如，公民登记能让用户完成投票、缴税等操作。依赖方可以是公共实体或私营企业。私营企业可在付费并获得用户同意后获取数据。

接下来是**联合认证**系统，一个身份提供者使用第三方为依赖方认证用户。除各种私营经纪商向服务订购方发出数字身份外，这类系统与集中身份系统相似。

最后，**分布式身份**系统将众多身份提供者与众多依赖方连接在一起。这类系统为用户设立数字「钱包」以实现各大网站和应用的通用登陆。通常情况下这类系统为私营，且依赖公共的操作准则，而非管理机构。

01 内部身份管理	同一实体既是身份提供者也是依赖方	最适于在单一实体内依据内部信息管理用户权限的情况，以确保正确的人有使用正确资源的权限
02 外部认证	多名身份提供者为单一依赖方认证用户	最适于简化用户使用单一实体所提供的一系列服务的情况，用户使用不同服务时无需重复登录
03 集中身份	一名身份提供者服务多名依赖方	最适于需提供不同用户完整、准确且标准化的非隐私数据的情况
04 联合认证	一组身份提供者为多名依赖方认证用户	最适于在为多个实体提供用户完整、准确且标准化数据的同时，用户可享受多个实体提供的服务且无需重复登录的情况
05 分布式身份	多名身份提供者服务多名不同的依赖方	最适于为用户提供在网络环境下便捷、可控且隐私受到保护的服务

指导原则

一个成功的自然身份网络应基于五大原则。

其一是社会价值。即身份系统应为所有用户提供身份，从用户利益出发并向所有有意参与的用户开放。与众多用户建立联系的金融机构可推动身份系统的建设，使其更具有包容性。

其二，身份系统应保护用户信息。目前的身份系统将用户置于危险境地，用户信息易遭遇隐私侵犯、数据泄露和过度曝光。数字身份系统应确保依赖方只看得到他们需要的数据且这些数据仅用于他们已披露的用途。对金融机构而言，即意味着身份系统应具有网络弹性且符合数据保护和储存标准。

这引出了下一项原则，即在身份系统中用户能控制个人信息的储存和传递。由于用户的不信赖，不止一个身份系统宣告失败。基于此，金融机构在使用或分享用户身份信息前须征得用户同意。

下一项原则是将身份系统视为可持续发展的长期业务。利益相关方应了解他们的投资终会有所回报。作为重要且值得信赖的私营实体，金融机构在构建系统的运行规定及准则时担当了重要的角色，这也是将身份即服务货币化的一次机会。

最后一项原则是按照开放的技术和数据标准建立身份系统。系统需具备可拓展性并能够服务于不断变化的用户需求。这意味着用户转换金融机构将更加便利。

建立成功的身份网络并不容易。你要考虑用户是谁？身份系统会解决哪些问题？你对这些问题的回答将帮助你决定要建立一个什么样的系统。面对其他问题时，考虑上述五项指导原则以及他们对金融机构的潜在影响将帮助你做出正确的选择。

数字身份之指引原则

- **社会价值**。系统能为所有用户使用并实现利益相关方收益最大化。
- **隐私提升**。用户信息只在恰当的情况下向正确的实体提供。
- **以用户为中心**。用户可控制他们的信息并决定谁有权持有和获得这些信息。
- **可行且可持续**。身份系统是一项可持续发展的业务且有较强的抗政治波动能力。
- **开放灵活**。系统依据开放的标准建立，以保障系统具有可拓展性和可开发性；系统标准和指导原则需对利益相关方保持透明。

好处

如果使用得当，金融机构以及其他相关方（包括：用户、身份提供者、依赖方、政府及监管方）都将获益于数字身份网络。

网络利益相关方

隐私

用户可控制谁有权访问其属性。

安全

用户属性存放于安全地点，依赖方知晓谁为合法人士。

透明

用户知道自己的属性何时以何种方式曝光。

便捷

数字属性迁移令用户交易更为便捷。

定位

通过与用户建立稳固的关系，身份提供者成为数字经济的重要组成部分。

紧密

流畅的用户体验打破了交易中的障碍。

服务

详细的用户信息有助身份提供者及依赖方为用户提供量身定制的产品及服务。

收益

依赖方简化了交易程序，同时身份提供者能够就交易收取费用。

风险

身份提供者及依赖方知道如发生数据丢失或违约他们将承担的责任。

政府及监管人员

流程

政府能够更高效地与市民互动，节约时间与金钱。

服务

政府更容易识别不同群体的公民并为其提供服务。

资产

监管人员更易追踪资产源头及所有权。

实体

监管人员可以将不同层级的法律实体聚合起来监督。

合规

监管人员能够访问可信的实时用户属性，整体合规程序得到优化。

数据

所有金融机构的数据采集与存储均是标准化的，从而避免数据融合时的冲突。

金融机构

服务

详细可信的客户信息有助金融机构为用户提供量身定制的服务。

运营

数字属性迁移及处理有助于金融机构简化并自动化操作流程，从而减少人为失误。

安全

安全的、数字化的信息存储减少了因信息被盗或认证破坏所产生的欺诈。

合规

数字属性处理及对用户身份更深入的了解使合规变得更容易也更精确。

收益

金融机构可以通过改善产品和服务，以及提供身份服务增加收入。

竞争力

金融机构可以提供流畅的用户体验，并将自身视为数字经济的重要组成部分。

未来应用

除其本身的优势外，数字身份在金融服务业务中有何特征？和其他新技术一样，这取决于在金融服务业中将如何应用数字身份。我们在此探索8种潜在应用。

量身定制的风险预测。金融机构使用预测算法及他们能够获得的所有客户信息来进行风险预测。未来，机构可以利用用户数字档案中已有的属性，连同一系列用户可能提供的其他属性来预测风险。随着更多更优质的信息可供使用，金融机构能够为客户提供量身定制的风险及信用产品，以此挽留客户。

国际迁移。倘若没有身份证明，任何人士都无法成功开立账户。如果金融机构能为客户建立没有财务历史的身份，有时金融机构为了争取业务，不得不为客户建立一个没有财务历史的空白身份。但如果用户有了数字身份，这种乏味的「白板」状况就能得以避免。在世界上任何地方，用户都可以凭借先前机构提供的证明及采集的用户属性，以获得新机构提供的金融服务或其他服务。而各个新机构又成为另一个身份提供者，这进一步强化了用户的数字身份。

与支付相关的属性。试想你再也无需在交易时手动确认年龄、货运信息或其他任何资料。数字身份通过允许商家从金融机构直接获得他们想要的资料（在取得用户许可的情况下），让这一切成为现实。属性的数字迁移避免了潜在的人为失误，可以帮助更多交易顺利完成。如果加入身份认证，那么潜在欺诈也将得以避免。

数字报税。目前，个人与企业必须在报税前从多方（包括金融机构、雇主、学校等）收集信息。但数字身份或许能够说服政府接受纳税人指定的金融机构的申报。金融机构能够利用其掌握的客户金融控股、资产、收入及个人环境的完整信息来自动化填写申报表。

厘定全部风险敞口。由于所有权架构复杂，尽职调查所需的工作量大，法律实体通常无法轻易厘定其在某项交易中的风险敞口。数字身份有助于对交易各方情况有一个总体了解，令公司能够更便捷地厘定自身面临的风险问题。

识别交易对手。如今几乎不可能识别经纪交易中的所有参与方。但如果有了数字身份，法律实体便能要求调查第三方的综合身份以及所涉资产的所有权。了解更多直接客户及终端客户的信息有助于就完成交易作出更知情的决策。

连接个人身份及企业身份。企业并不一定会与所有与其相关联的人士联系在一起。如果个人以及法律实体的身份属性均通过标准方式实现数字化采集、存储以及迁移，金融机构便能可靠地洞察他们的关系。精确、实时的资料有助于了解客户并实现其他目的。

追踪总资产再抵押。当资产被再抵押时，其交易与所有权历史将变得模糊，这会产生交易对手风险，并难以厘定资产的公允价值。此外，因缺乏历史追踪机制，资产再抵押程度难以被限定。统一、标准化的数字资产信息令查询资产发行人及交易历史成为可能，从而有助于防止过度的再抵押，降低交易的整体风险。

结论

会出现单一的全球身份解决方案吗？不要有所指望。只要我们拥有建立及联系身份网络的基础原则，这就可能毫无意义。

一方面，不同类型用户的身份需求各不相同。个人用户的诉求是能够安全便捷地完成交易。法律实体需要一个能够汇总数据以管控风险的综合性解决方案。对资产而言，则需要有一个追踪体系使其所有权及价值透明化。

另一个不同点体现在隐私方面。个人用户必须有隐私。法律实体及资产可以没有；实际上，隐私甚至可能对其实现更大目标形成阻碍。在任何情况下，个人用户拥有自主权，而法律实体以及资产有代其行事的托管人。

此外，身份具有文化属性。某些国家的国民拥有身份证，而另一些则没有。一些政府可能不够稳定，所以无法实施数字身份。

因此并没有万全之策。不同的群体会建立自己的身份网络，也许本该如此。即便如此，在最高层面上，所有网络都遵循着同样的发展路径：

01. 了解服务对象是谁。

02. 理解系统需要满足的需求。

03. 决定令系统运作必须参与的各方。

04. 找寻合作方式——不论采取私营合伙、财团、公用事业或其他形式。

05. 描述解决方案必须具备的功能，并将其转化为系统开发人员能够实施的技术需求。

06. 整合解决方案、测试并启用系统。

我们鼓励金融机构考虑有关数字身份的自下而上的解决方案。首先，与众多参与方共同测试并完善系统，随后逐渐扩大其规模，以纳入更多用户、依赖方以及身份提供者。

金融机构作为团体能够做的另一件事是：建立网络间的连接器。这将允许数字身份网络在其自然边界内形成，以最佳方式永久服务于各方。连接器是实现互操作性的桥梁——它们令数字身份的全球蓝图得以成型。

联系方式

德勤中国

白杰庭
中国金融服务行业主管合伙人
香港
+852 2238 7819
tpagett@deloitte.com.hk

施仲辉
银行及证券行业 (中国大陆) 主管合伙人
北京
+86 10 8520 7378
mshi@deloitte.com.cn

文启斯
保险业 (中国大陆) 主管合伙人
北京
+86 10 8520 7386
bman@deloitte.com.cn

秦谊
投资管理行业 (中国大陆) 主管合伙人
上海
+86 21 6141 1998
jqin@deloitte.com.cn

Robert Rooks
银行及证券行业 (香港地区) 主管合伙人
香港
+852 2238 7863
rrooks@deloitte.com.hk

胡伟杰
保险行业 (香港地区) 主管合伙人
香港
+852 2238 7248
davidwwu@deloitte.com.hk

刘明扬
投资管理行业 (香港地区) 主管合伙人
香港
+852 2852 1082
antlau@deloitte.com.hk

全球联系人

Bob Contri
德勤有限公司
金融服务全球领导人
纽约
bcontri@deloitte.com

Rob Galaski
德勤加拿大
金融服务行业未来论坛 德勤领导人
多伦多
rgalaski@deloitte.ca

Cary Stier
德勤有限公司
投资管理全球主管领导人
纽约
cstier@deloitte.com

Neal Baumann
德勤有限公司
保险全球领导人
纽约
nealbaumann@deloitte.com

Joe Guastella
德勤有限公司
金融服务咨询全球领导人
纽约
jguastella@deloitte.com

Vikram Bhat
德勤美国
金融服务网络风险服务全球领导人
纽约
vbhat@deloitte.com

Anna Celner
德勤有限公司
银行业&证券全球领导人
苏黎世
acelner@deloitte.ch

Ted DeZabala
德勤有限公司
网络风险服务全球领导人
纽约
tdezabala@deloitte.com

地区联系人

美洲

Rohit Malhotra
德勤美国
rmalhotra@deloitte.com

Linda Pawczuk
德勤美国
lpawczuk@deloitte.com

Andre Romanovskiy
德勤加拿大
aromanovskiy@deloitte.ca

欧洲、中东及非洲

Michel De La Belliere
德勤法国
mdelabelliere@deloitte.fr

Nick Seaver
德勤英国
nseaver@deloitte.co.uk

Chris Verdonck
德勤比利时
cverdonck@deloitte.com

亚太

Trey Gannon
德勤澳大利亚
tregannon@deloitte.com.au

Mitsuhiko Maruyama
德勤日本
mitsuhiko.maruyama@tohmatsu.co.jp

Tse Gan Thio
德勤东南亚
tgthio@deloitte.com

特别感谢德勤加拿大Christine Robson对本报告的帮助。

Deloitte.