数字身份

# 在数字时代重建信任

2019年3月

万事达卡

# 目录

# 摘要

**本篇报告主要展现了万事达卡对于数字交互未来发展的洞察，描述了信任在其中发挥的作用以及万事达卡将数字身份视为信任基础的原因。本文提出了一种高效且包容的数字身份业务模式，其本质是协作与联结。同时，清晰地定义和建立了在由可信参与者组成的构架中各方的角色和价值，将万事达卡数字身份原则作为所有系统模型、设计和服务实施的核心。**

## 本文关键内容有：

- 全球范围内，个人是所有数字交互的核心
- 为此类数字交互创建明确的框架
- 介绍高效的数字身份系统的工作原理
- 展示万事达卡在多个利益相关方的生态系统中的合作地位
- 为依赖数字身份的客户和支持该系统的合作伙伴创造最大价值

我们认为，数字交互应该是隐私性有保证，安全、智能且高效的。这些数字交互将通过以用户为中心且由个人管理和控制的数字身份实现，数字身份可以让用户与参与的组织之间进行交互。可重复使用的数字身份服务，需要建立在对数字身份的充分认识、信任和用户参与之上。万事达卡建立的系统模型以用户为中心，严格遵循隐私保护原则，不需要进一步汇总身份数据或构建新的集中式数据结构。

## 我们设想了一种简便、智能且安全的数字身份服务：

- **简便**：让用户和第三方之间可以轻松、安全且充满信任地进行数字交互
- **智能**：只需最低程度的数据交换即可实现数字交互
- **安全**：有效保护和使用数据，并由合法所有者管控数据

协作是万事达卡数字身份服务的核心。任何政府、科技公司、金融机构或产业部门都无法单独高效地提供数字身份服务，因此需要通过共生、合作、协同来实现单方面无法实现的目标。万事达卡正在构建良好的伙伴关系、投入广泛的资源，并充分利用我们的网络资源来实现数字交互的未来发展目标。

我们认为，基于协作的生态系统是未来管理数字交互的最佳业务模式。正如我们目前助力消费者、商户和金融机构以安全、方便和信任的方式进行交易和交互一样，在数字身份领域万事达卡将自己视为赋能者。我们也已经与政府、银行、电信公司以及其他主要的身份数据拥有者展开了密切合作。

万事达卡不会留存个人身份数据，但会有效地满足对个人身份数据有服务需求的相关方及其用户。万事达卡数字身份系统符合各国相关标准并具备全球协同性，其允许需求方明确定义其身份验证需求。

接下来，我们将介绍该模式的运作。

# 数字交互

我们正在塑造一个用户及其移动设备可以无缝、流畅且充满自信地与其他人或机构进行数字交互的世界，一个可以轻松建立信任的世界：人们可以很容易地通过身份识别获得他们想要的服务或体验；一个人们可以通过语音、触摸和体感，实现从个人电脑和智能手机到联网家庭、汽车和可穿戴设备联结的多维数字交互世界。

当今出生的这一代也许没有银行卡、护照或现金，她第一次支付使用的设备很可能是她的手机、手表或一件衣服，她的签名可能是指纹、人脸或声音。归根结底，她自己就是她的身份证明。

从某种意义上说，这是传统身份认证和信任概念的回归。个人可以通过视觉、姓名、口音或其他身体特征被识别，并在必要时由受信任的第三方担保。但现在随着数字交互的日益增加，不仅是我们自己在频繁使用我们的身份信息，我们所持有的设备也常常代表我们在不断进行使用。

物理世界和数字世界的融合造就了这一局面，如今我们处在被一个互联网包围的时代，一个超链接的时代，一个数字服务与日常生活融为一体的时代。这给消费者、生产者、公民甚至全人类整体都带来了巨大的好处，数字服务改变了人们购物、经商、参与政治、就医乃至沟通的方式。

# 建立信任

我们当前对信任的定义是：
与未知方之间的确信关系[1]。

数字世界充满了未知，但是提供数字服务的组织以及与之互动的人，需要信任其所在的交互环境。要实现这种信念的飞跃，必须以信任为系统的核心。

数字身份即是在交互的两端建立信心和信任，每一方都需要确信另一方的真实身份。另一方面，双方都需要数字系统中的信任来支持这种交互。

试想一下这样的世界：每个人的身份和代表其身份的设备可以在多个触点以及数字和物理世界中迅速、安全且可靠地得到验证；无需密码即可获得访问权限，只有经过同意才能交换数据；简单到就像说一句：“嗨，这就是我。”这就是万事达卡正在努力创造的未来世界。

# 赢得信任

你如何相信一个素不相识，看不见摸不着，又无法亲自现身说法的人？

传统意义上的身份识别，无论是出示护照，提供住址，出示驾驶证或者当面查验，其实都是限定在物理世界的验证机制。想象一下你在线上积累的数百个账户、密码和需要记忆的（或容易忘记的）的数据，在超过50亿人在线的数字世界中，数字认证的工作量是多么繁重且不牢靠。

一位普通用户可能需要管理150个登录账号，[2]每个账号都有不同的密码和身份验证方式。愈演愈烈的线上欺诈已经成为比线下欺诈更为严重的问题，而且在物联网世界中，这些风险还在成倍增加。在未来几年内，全球连接的设备和传感器将达500亿[3]个，每个设备和传感器都会给使用者带来潜在的安全威胁。

然而另一方面，目前还有超过10亿人没有被身份认证系统所覆盖。由于他们的住址太偏远或难以联系，加上本身缺乏与主要机构和政府的互动，身份认证系统很难为他们提供服务。

很显然，人们需要一个经过验证且能够被世界各地、不同交互类型的数字终端接受的身份，一个不需要在脆弱的数据库中进行数据加工，且完全由个人控制的身份。例如，成年人可以在不透露出生年月的情况下就能证明自己可以购买有年龄限制的产品，他们也可以在没带驾照的情况下租车，不用携带护照外出旅游或是在没有纸质银行对账单的情况下获得抵押贷款。

那么到底是什么阻碍了便利的数字认证呢？目前，一些国家已经开发了适用于本土的数字身份系统，但不同国家之间往往存在着迥然的差异，构建一种适用于所有国家的数字认证系统是我们面临的巨大挑战。

如今，没有人会在不同的商店或国家使用不同的信用卡，现代科技的发展使得数据可以在银行、商家、政府和消费者之间实现安全交换，只要一张信用卡足矣。同样的，要使得数字身份发挥更大的作用，也需要具有商业意义的创新、标准、协同性以及利益相关者之间的信任。

# 赢得信任

## 关键问题

### 用户

我们用来与政府进行互动、获取服务和支付商品的身份往往是非常脆弱的。通常只需要破坏一个数据库就可以窃取身份信息并实施欺诈。目前，人们必须向不同代理机构重复地提供大量的个人信息，这些信息提供的次数越多，被泄漏的风险就越大。用户为了保护自己的身份数据、信用和财产安全，不得不同时使用多个密码，但他们对个人身份数据又缺乏管控权。与此同时，如果相关管控权真正得到落实，那么透明度往往又会变得很低。

### 组织

简便、安全且可靠的数字身份验证方法的缺失，常常会造成交易摩擦、增加欺诈、泄露隐私并限制对服务的获取。

### 包容性

世界上还有很大一部分人无法通过可信赖的身份认证来证明他们是谁，而这些人往往又最需要身份认证。最贫穷的那40%人口获得的身份验证机会也最少[4]，他们中还有超过10亿人缺乏最基本的且可验证的出生证明，游离于整个“身份网络”之外。联合国曾表示，没有官方的身份认证，也就无法享受金融、健康、公民以及数字化等各方面的普惠权益[5]。

### 数据泄露和身份信息盗窃

仅在美国，2017年就有1670万用户遭遇了身份相关的欺诈[6]，涉案金额达到168亿美元，同年相关数据泄露事件的数量也增加了44.7%[7]。大多数的数据泄漏都与身份信息盗窃案件相关[8]。2016年，犯罪分子通过整合多项个人真实数据，“合成”看似真实的假身份，共造成了60亿美元的损失[9]。

# 定义数字身份

2018至2019年，万事达卡组织了来自世界各地的权威专家和相关人士参与研讨，探索数字身份带来的机遇[10]。这项工作对我们与政府、合作伙伴和其他利益相关方的日常沟通以及我们在身份认证领域的长期专业积累做了有益补充，更帮助我们完善了对数字身份的定义。

我们将数字身份视作定义个人身份的数据整合，其核心是当与个人身份绑定时，能够在用户的控制下安全地访问和验证。数字身份的主要目的不只是识别某个人，更重要的是确认他们的身份是否有权访问相关服务或执行特定任务。

## 我们认为，数字身份应当是：

- 实时更新、高保真的、可用来定义个人身份的数字信息的整合
- 是动态的，多用途的，可重复使用的
- 是一种信息验证的方法，以获得授权享受服务，执行任务或获得权益
- 基于由分布式数据源（如金融机构、移动网络服务商和政府）组成的动态网络，根据需要发起验证

## 数字身份可包括：

- 姓名，出生日期，地址
- 生物特征（如指纹、面部信息、语音）
- 社会属性（如护照号码、社保号码）
- 职业认证（如医生、飞行员、大学学位）
- （如来自金融机构、零售商、移动网络商）等的动态数据交互

## 数字身份不仅仅是：

- 数字化的护照、驾驶证或身份证
- 密码的替代品
- 线上个人资料

# 数字身份原则

## 对个人的承诺


目前，人们通常需要付费以完成涉及数据和隐私的数字交互。人们每天都需要提供个人信息来获取基本的数字服务。他们通常不清楚数据存储的位置、安全性、以及可能后续被买卖的过程以及获益方。这对于个人来说，是一个非常不利的处境。

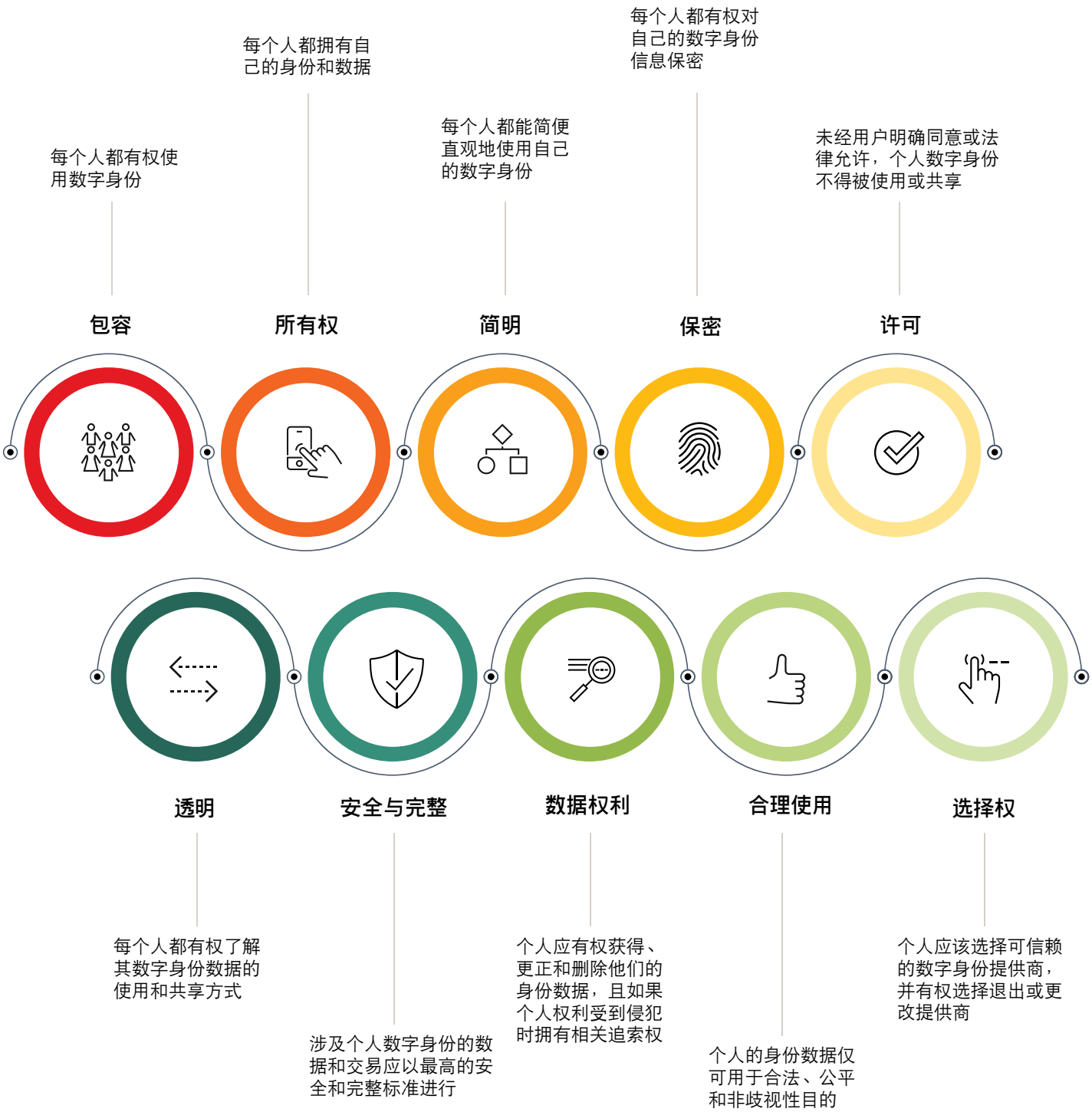
包括欧盟通用数据保护条例在内的多项隐私条例的发布，正在帮助大家重获信任，并为现代身份基础设施提供了一个良好的环境。

万事达卡认为，数字交互的系统框架非常重要。我们已经起草了数字认证原则作为指导方向，用来帮助用户管控数据并解决包括隐私、所有权、信息透明、安全性及其他方面可能存在的问题。

我们将此归结为：个人拥有其数字身份并有权管控自己的身份数据。

# 数字身份原则

## 万事达卡数字认证原则



# 数字身份原则

## 以用户为中心

万事达卡认为，便捷与隐私这两者并非不可兼得。我们所专注的数字身份服务在面向全球的同时也积极应对本地需求，其致力于实现机构与部门之间的协同性，并确保每个人都能成为其数据的守护者。

数字身份远不只包含创新的技术，它也定义了数字世界中的每个个体。因此，我们需要一个原则性框架和一个支持性的商业服务作为支撑。万事达卡认为，将个体置于数字认证生态系统的中心至关重要，我们的指导原则可以在促进信任和理解的同时，完善个人对数据的管控。

**使用以用户为中心的数字身份将为人们在与企业、服务提供商和社区互动时提供全新的、更优的客户体验，它们包括：**

- **金融服务**：在用户申请开立银行账户、贷款或支付账户时，改善并加快申请人识别流程
- **商务交易**：无论是何种支付类型、交易设备或服务提供商，用户都可以通过线上远程或在线下实体店内获得更加个性化和高效的购物体验
- **政府服务**：简化用户与政府机构和服务商之间的互动——例如报税、申请护照或领取福利等
- **国家福利**：验证福利分配并减少欺诈
- **健康服务**：在确保用户管控权的同时，改善服务提供商之间数据服务的互联互通
- **数字服务**：提供电子邮件、社交媒体、电影或音乐等流媒体服务和拼车共享平台用户更简化、更顺畅的使用流程
- **物联网**：保证设备和传感器能够代表用户或与用户安全地进行交互操作

# 数字身份原则

## 负责任的系统设计

**我们正在改变人们在数字世界中建立身份证书(认证信息)的方式：**

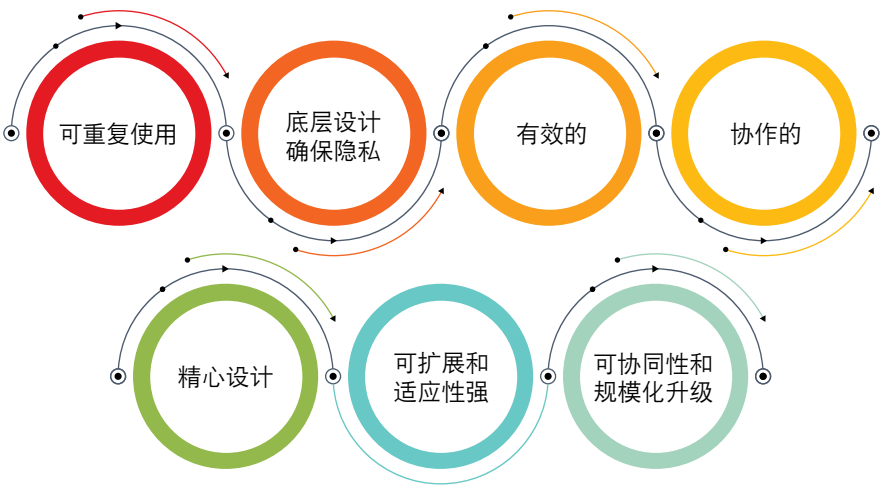
由特定、狭隘和封闭的系统，**转向透明的、全球协同性的服务**

由透明度低的数据过度共享，**转向由用户管控的数据共享**

由静态身份认证数据，转向动态和**生物特征的身份识别数据**

由数百种易受攻击的密码，转向可在**任何地方使用的且可重复利用的数字身份**

由将贫困人群排除在外的选择性系统，**转向面对所有人的包容性系统**




**万事达卡认为，实现这些转变的最好办法是按照我们的原则和核心目标设计一个负责任的系统:**

- **可重复使用的数字身份**：无需多个密码和身份验证程序，数字身份可以允许用户使用单一手段在多个数字服务（包括网站、应用程序和设备等）中进行身份验证
- **底层设计确保隐私**：确保用户在数字化生活中的数据隐私和管理数据身份时的透明度
- **有效性**：助力推出新的增值服务，在提高用户参与度、消除交易摩擦、降低身份认证服务成本和提高安全性的同时，满足监管要求
- **协作**：携手技术和运营方共同制定标准和规则
- **精心设计**：用分布式数据协同共生的生态系统取代传统的数据聚合方式
- **可扩展性和适应性强**：围绕一个核心进行系统构建，可以根据当地的标准、法规进行全部或部分部署
- **协同性和规模化升级**：为个人提供顺畅的数字交互，实现官方数据基础设施与私有企业数据验证参与方式之间的安全交互，同时满足本地市场对功能、性能、安全和其它相关法规的要求

# 数字身份应用

在现代生活中，每个小时都有数以百万计的身份验证或身份授权请求发生。它们或许很简单，比如登录个人电脑；也可能会很复杂，比如申请抵押贷款或签证。无论是在哪种情况下，一个可重复使用的数字身份都将构建一种全新的机制，显著改善个人和服务提供商所寻求的数字服务体验。

# 数字身份应用

## 案例分析

### 减轻验证压力

人们重视速度和便利性的同时也期望安全性能得到保证。这两者并非不可兼得。数字身份只获取并显示每个任务所需的认证信息。想通过登录网站或应用程序进入数字门户？数字身份可以像说“嗨，这就是我！”一样轻松地实现认证。想要登机？不用护照，指纹就可以了。从邮局取包裹？没有证件也可以！

通过安全地访问可靠的来源，调取最少的数据，数字身份能确保个人在不透露非必要数据信息的情况下获得特定服务。在风险较低的地方，证明个人身份很简单；对于用户的银行经理或医生来说，面对面的认证就已足够可靠。数字身份将这种简便的识别应用于数字交互领域，而复杂的核验流程则用于风险性更高的交互，例如证明抵押资格或访问医疗记录等。

案例

Ella采用不同的方式使用她的数字身份。在酒吧，她用数字身份来证明自己年龄符合买酒要求，无需出示可能会泄漏个人姓名、地址和出生日期等信息的驾照。她使用自己的数字身份进入办公大楼，而不用员工卡。她可以使用数字身份在线订购处方药、参加会员奖励计划、订阅杂志、注册相亲网站、创建社交媒体档案以及分享最喜欢的音乐等。Ella可以自由决定在何处使用她的数字身份，提供哪些数据以及向谁提供。

## 制定具有全球协同性的本地化解决方案

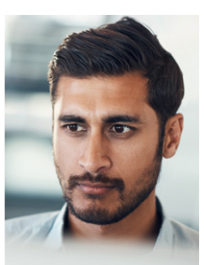
印度、爱沙尼亚、加拿大、比利时和一些北欧国家已经采用了数字身份平台。但是这些平台既不是全球性的，也不具备协同性。除了政府部门间的应用外，这些平台能起到的作用非常有限，甚至根本起不到作用。如果没有商定的统一标准且不具备协同性，就无法将数字身份平台扩展到自身以外的区域进行部署。万事达卡认为，本土化解决方案也可以实现全球范围内的交互，平台规模对于实现包容性至关重要。为此，万事达卡正与各国政府密切合作以制定此类本地化解决方案。

案例

移居国外后，Michael开始了新的工作。为了在当地开立银行账户他需要一个当地地址，但在租公寓时他却需要提供当地银行账户，两个需求之间相互矛盾。而凭借全球认可的数字身份，他可以通过自己的信用记录证明自己是谁，提供以前的工作信息验证个人信息。

## 减少欺诈

由于现行通过数字渠道验证身份的方法往往不够简便、安全和可靠，不仅增加了网上交易的摩擦，降低对隐私的保护，限制了用户获取服务，更使其成为滋生数字欺诈的温床。网上交易的欺诈率比刷卡高出了四倍[11]。数字身份可通过技术方法解决这些问题，其准确水平已达到全新的高度，并且支持跨设备和跨平台工作。



案例

Rahul是信用评级机构重大数据泄露事件的受害者，犯罪分子盗取了他所有的身份认证数据：包括姓名、出生日期、密码和其他关键信息。犯罪分子利用这些数据开立了新的账户并申请了贷款，从而损害了Rahul的信用记录。现在他有了数字身份，评估贷款所需的数据不仅不再存储在单一的地方，而且只有在他本人的许可下，才可以根据实际需求安全地提供其个人数据。

## 优化交易流程

日常商务往来中会涉及身份信息的方方面面。数字身份可以显著减少电子商务中的摩擦，有助于实现“一键式”开账，有效地简化“了解你的客户”（KYC , Know Your Customer）流程和新用户启用服务的流程。

案例

由于网上账户太多，Jemma经常记不清各个账户的用户名和密码。凭借数字身份，她可以快速、轻松地登录所有账户，“一键式”完成账户创建并通过地址和年龄验证。近期，她开始了一个新工作并需要开立新的银行账户，利用数字身份，她只需提交极少的材料，就迅速而安全地完成了入职和银行账户开立这两项任务。

## 包容性

身份，是我们在世界上合法生存的证明，它可以证明我们是谁，并且明确我们作为公民所拥有的权利。然而，世界上仍有超过10亿人身处“灰色地带”，缺乏最基础的，可供核验的出生证明。那些未能获取官方身份证明的人们无法享受其所在国家提供的相应服务，也无法开立银行账户甚至就医。此外，拥有数字身份的人群和没有数字身份的人群也往往存在着社会及经济状态的明显分野。为了改善此种状况，联合国可持续发展委员会在可持续发展目标（SDGs, Sustainable Development Goals）16.9中提出，计划于2030年前为所有人提供合法身份。

数字身份为包容性提供了快速、高效且可有效防止欺诈的解决方案，让更多人享受各种服务及福利。在欺诈案频发且犯罪记录维护堪忧的地区，数字身份尤其能显著改善人们的生活，打击欺诈、人口贩卖和其他有组织的犯罪行为。

案例

作为一个收入有限的母亲，Anya有权得到国家的财政援助。但她因为之前一直没有官方机构认可的身份，所以无法享受相关援助。然而，通过注册数字身份，Anya就可以直接获得补助金，这笔资金被汇入由Anya的指纹作为密码保护的预付借记卡上。此外，Anya还可以利用同一数字身份开设银行账户和预约就医。

# 协作体系

## 在身份认证交易中建立信任

多年来，我们到底是如何判断和核实身份的?

有人可能会这样回答：“我是Bob，1985年9月29日出生于悉尼，这是我的居住地址。”但是，不认识Bob的人需要通过那些认识和信任Bob的人来验证他的陈述是否属实。而认识和信任Bob的人，其实就是支持Bob的一个或多个第三方。万事达卡数字身份系统将不认识Bob的人统称为**需求方**，将认识和信任Bob的人称为**身份验证方**。


要将这个三方关系转变为有效的数字身份体系，用户还需要必要的工具来管理和出示他们的身份数据。现实中，数以百万计的用户、需求方和身份验证方需要进行彼此交互，关系的协调就显得尤为重要。

为应对这些挑战，万事达卡引入了另外两个角色：**信任提供商和数字身份服务提供商**。在理想情况下，信任提供商与用户间有预先存在的信任关系，比如品牌可以充当数字身份服务的桥梁。信任提供商还可以为用户提供注册、使用和管理数字身份的服务。

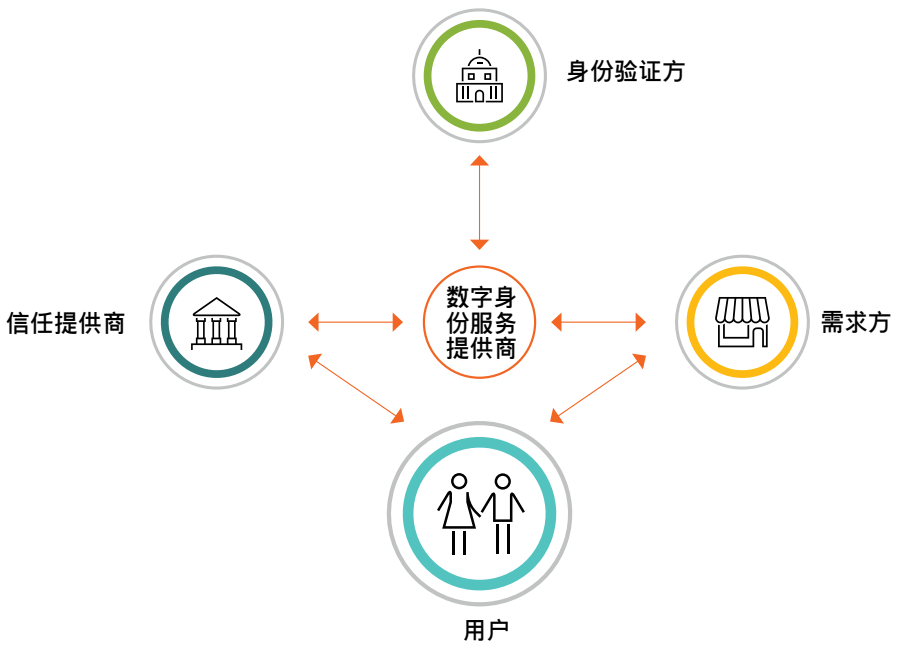
**数字身份服务提供商**则提供各种服务，负责建立数字身份网络中的技术交互、价值和经济利益交换、服务水准协议以及责任分担，并为数字身份服务创造商用空间 。

信任提供商、身份验证方和数字身份服务提供商协同运营的身份验证网络，其广泛的用户覆盖是任何单一机构都无法与之媲美的。

# 协作体系

## 数字身份系统的角色

- **用户**：提交身份识别信息
- **需求方**：依赖用户提供的身份识别信息进行验证
- **身份验证方**：验证用户提供的身份识别信息
- **信任提供商**：为用户提供服务和工具
- **数字身份服务提供商**：负责安排协调服务、组织市场、建立标准




基于不同的角色分工，数字身份系统可以使现有利益相关方有效地与关键参与者（即用户和需求方）进行交互并传递价值。它是一个以用户为中心的分布式数字身份系统，以及附加的各参与方利益和动机保持一致的商业框架。

**主要特点**：

- 用户不能独自确定数字身份，需求方需要通过多个身份验证方的确认
- 通过设定商业框架的相关业务角色鼓励身份验证方参与
- 用户需要通过APP等工具来使用数字身份，而信任提供商（如银行或移动网络运营商）可以充当工具提供方
- 引入信誉良好的数字身份服务提供商，使所有参与者具备足够信心，并能够在复杂的数字环境中获取应有的帮助
- 针对用户的身份及其数据，需求方可以通过高性价比且可扩展的方式，获得简洁且值得信赖的担保

# 协作体系

## 传递价值

万事达卡致力于将利益相关者聚集在一起，创造只有通过合作才能实现的协同效应。万事达卡数字身份系统的主要优势有：

**以用户为中心的数据**：该系统模式在用户移动设备上存储个人数据，进行验证并保存使用结果。具备优秀韧性的分布式基础结构，摒弃了集中储存身份数据的需求。

**角色导向**：该模式同时负责分配功能和职责，使金融机构、移动电话运营商、政府、邮政部门和其他利益相关方能够在费用和风险最小化的情况下充分发挥各自的优势。

**身份验证方**：最适合该系统的身份验证方，是那些拥有用户数字身份属性最终确认能力的权力方。例如出入境管理部门是最适合进行护照数据有效性验证的机构，邮政服务机构是验证地址有效性的首选，移动网络运营商是验证智能手机设备详细情况的第一选择。选择最适合的验证方可以提高系统运作效率，获得其他利益相关方的信任。金融机构、移动网络运营商、邮政服务、教育机构和政府等机构也拥有其用户的信任，这使得他们有资格参与到该系统的运作中，并担任有实质作用的角色。

**信任提供商**：在许多地区，用户与零售银行的数字关系代表了一种理想的用户与信任提供商的关系。智能手机银行应用程序的用户也倾向使用数字身份，因为银行已经进行了一些必要的安全投资进行用户信息验证，使之成为用户最值得信赖的信任提供商之一。在不同的市场和用户群中，像移动网络运营商、邮政部门甚至大学等都可以成为合适的信任供应商选择。

**需求方**：建立该系统的目的，是弥合需求方与用户间（特别是数字交互方面）的信任缺口。需求方是系统中的主要客户，他们支付费用获得经验证的身份信息和后续的身份验证服务。

**政府**：政府通常制订个人身份的国家标准。通过与私有企业合作，政府可以提供高效、公平和合规的数字身份服务，为用户和组织实现互利共赢。政府也可以通过从向公民提供低成本、高质量、易获取的服务中获益。

**多角色**：系统中的参与者可能扮演多个角色。银行可以在充当信任提供商的同时担任身份验证方（根据账户开户数据），同时银行也可能发起数字身份验证，这样银行就成为需求方。政府可以充当身份验证方，也可以作为需求方获取数字身份验证服务。

**不同的交互模式**：虽然数字身份认证可以在数字技术的帮助下通过面对面的形式完成，但在大多数情况下，类似操作都是远程进行的。在这种情况下，系统必须能够确认用户是身份的拥有者本人，而不是一个机器人或意图欺诈的罪犯。

**性价比最优**：由于每个参与者都扮演着最适合的角色，对于所有参与者来说，建立数字身份系统的成本将降至最低。

# 技术和标准所扮演的角色

## 核心技术

虽然目前我们拥有创建有效数字身份生态系统所需的核心技术，但更具挑战性的问题是如何在确保效率和有效性的前提下，合规地利用这些技术。万事达卡在将技术进行可扩展、高适应性和合规应用方面拥有丰富的经验，确保数字交互在可信的基础上进行。

**生物识别特征**

身份认证市场的发展弥补了静态身份数据的弊端，道德层面上合理使用生物识别数据变得越来越重要。用户生物识别数据的验证、动态识别和相关安全处理，是技术创新和应用密切关注的关键领域。

**安全体系**

现代加密手段和密钥管理方法的使用对于建立体系内的信任至关重要，包括在验证过程中保护身份数据，确保身份验证申请完整性，保护用户掌握的数据，并确保整个体系中所有设备、云服务、分布式账簿服务和各方接口间都采用逐级加密的技术。

**终端设备**

该体系必须考虑全球 75 亿人当前和未来的需求，涵盖在智能数字网络中运行的各种设备的数字交互。健全系统服务设计的核心是通过加密和生物识别技术保护这些终端设备，并确保用户身份数据的隐私保护能得到强化。

**分布式账簿技术**

基于区块链的安全分布式技术可以提高数字交互记录透明度且杜绝篡改，因此可抵御拒绝服务型攻击（DoS, Denial-of-Service）。与此同时，值得进一步考虑的是如何以保留核心安全功能和充分尊重隐私原则的方式应用此技术。

# 技术和标准所扮演的角色

## 标准

### 框架

现行关于隐私和公开数据的法规，为有效的数字身份服务提供了支持性框架。国家和区域性机构（例如电子身份识别和托管服务条例(eIDAS)、美国国家标准与技术研究所(NIST)和其他一些机构）也正在继续深入开展相关工作。监管机构应确保继续支持私有企业的商业化参与并不断鼓励他们创新。此外，为了确保数字身份得到广泛采用，我们必须建立相关技术标准。就此，万事达卡尤其感谢全球去中心化身份联盟（Decentralized Identity Foundation, DIF）、万维网联盟（Worldwide Web Consortium, W3C）和开放身份联盟（Open ID Foundation）分别在分布式标识、可验证声明和推动开放身份标准等方面所作的不懈努力。

### 协作

协作不仅对于建立商业化和可运营的数字身份基础设施而言很关键，在技术的使用上也尤为重要。目前，万事达卡正在与业内一流的技术伙伴合作，构建和开发世界一流的数字身份服务。

### 扩展

我们的系统兼容现有身份数据提供商和各国的身份计划，并且充分支持医疗和金融服务等领域内那些依赖第三方身份认证的应用程序。

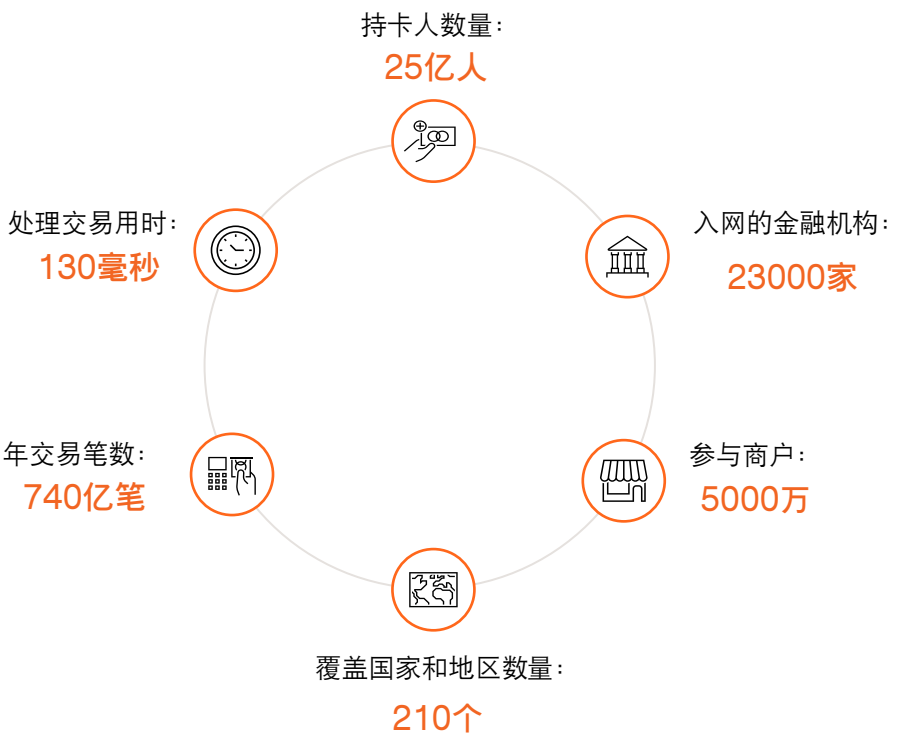
# 万事达卡的角色

半个多世纪以来，万事达卡与各界合作伙伴始终致力于开发一种可以将消费者、商家、金融机构、政府和技术提供商充分联结的支付模式。

这与全球数字身份服务所需的复杂多方协调，有很多明显的相似之处。在支付领域中，身份的交换意味着消费者和商家开始互动。世界经济论坛认为，目前全球金融行业所使用的交易框架是最接近可协同性身份识别及验证系统的事物[12]。

万事达卡投资构建了可靠的数字交互生态系统，我们致力于打造可以覆盖所有人的新型身份认证系统，不仅更安全、更包容、更便捷，还可提供更高级别的隐私保护。

此外，基于万事达卡在管理和运营网络方面的经验，对普惠金融的关注，对数据隐私的敏感度和投资全球基础设施的承诺，我们被视为使用数字身份的坚定拥护者。万事达卡将不断优化服务平台和网络，协助制定运作和管理规章，建立跨网络合作，吸引并服务各方客户和合作伙伴。



# 万事达卡的角色

## 万事达卡主要资产

| | |
|---|---|
| **全球协同性** | 万事达卡所设计的身份认证网络拥有可以覆盖全球200余个国家和地区的跨境协同性，使得一个国家的用户数字身份能在另一个国家或地区使用。 |
| **包容全球服务提供商** | 作为在本地市场运营的国际品牌，可以通过寻求全球公认的数字身份服务提供商来扩大规模和覆盖范围。 |
| **网络基础设施和治理** | 凭借在构建和运营大型全球支付网络方面积累的专业知识，万事达卡能够为数字身份提供可扩展的网络服务。在携手利益相关方制定网络体系规则、起草法律合同和配合监管这些关键职能领域，万事达卡同样处于领先地位。 |
| **高效的系统模型** | 万事达卡通过使用多个权威的身份属性验证源，构建了高效的系统。通过利用网络中每个利益相关方基于其现有核心业务和数据资产产生的优势，该模型将传递身份信息的成本降至最低，从而加快了市场推进的速度。 |
| **用户选择权** | 通过启用由多个信任提供商组成的网络，万事达卡从开展业务初期就为用户提供了广泛的提供商以供选择。 |
| **投资与承诺** | 万事达为所有网络参与方投资开展了一项商业计划，包括金融、技术、责任、安全、隐私和运作规章。从规模上讲，此项计划是全球性的，具有协同性并能做到因地制宜。 |
| **市场创建者** | 万事达卡在全球拥有由 5,000万家商户组成的支付网络，在鼓励市场接受数字身份方面拥有很大优势。 |
| **支持全球服务提供商** | 通过利用现有全球网络的支持基础设施，万事达卡可以用最低的成本支持身份识别网络。 |
| **安全与隐私体系** | 万事达卡数字身份原则充分体现了对用户、客户和合作伙伴的承诺。 |

# 结论

目前，技术变革正在以前所未有的速度进行。车轮、印刷机的发明和第一次载人航天飞行的时间相隔千年，而互联网、智能手机、芯片技术和个人电脑却在极短的时间间隔内，极大地改变了世界。

纵观历史，数字交互的演变不过眨眼之间，这不可避免地向我们在传统世界中对身份、信任和隐私的认知发起了挑战。

现有涉及数字身份的各种概念往往无法应对这些挑战，因为它们不够安全，相互不兼容或缺乏树立用户信心所必须的信任。而精心设计且可互操作的数字身份系统可以为我们提供安全、有保障和可靠的数字交互。现有网络为促进可信数字金融交易而不断发展的基础设施，则为实现这一目标提供了基本模型。

此外，使用一套从一开始就让用户对自己数字身份负责的原则来支持数字交互，同时赋予交互对象足够的信心，尤其至关重要。

只有利益相关方和创新者在数字身份领域携手并进，才能共同将这套系统真正建立起来。鉴于这项工作如此重要，没有任何一个机构能够拥有足够的方法、基础设施或市场地位可以独自胜任，也不应由单一的机构承担这一责任。

# 专业术语表

**去中心化身份**：一种身份认证系统模型，将身份的所有权归属于个人。

**全球去中心化身份联盟**：一个致力于研究创建去中心化身份开放式生态系统的组织。

**数字发卡**：直接在移动钱包中植入信用卡/借记卡功能。

**数字身份**：用来确认经验证的用户或其他主体身份的数据集合。

**通用数据保护条例(GDPR)**：欧盟通用数据保护条例EU 2016/679是由欧洲议会、欧洲联盟理事会和欧洲委员会共同制定的，为加强和统一欧盟内所有个人数据保护的一项规定。

**电子身份识别和托管服务条例(eIDAS)**：通常简称为EU 910/2014，是由欧洲议会和欧洲联盟理事会共同制定的，关于联盟内市场电子交易中的电子身份识别和托管服务的条例。

**身份认证**：认证用户身份的过程。

**身份验证服务提供商**：一个能够验证用户身份数据的权威组织，例如政府（验证护照）、移动网络运营商（确定手机定位）、邮政服务（确定地址）、金融机构（获取客户认证操作中的核心身份数据）。

**物联网**：一个由相互关联的计算设备、机械和数字机器、对象、具有唯一标识符的人组成的系统，这个系统中不需要人对人或人对计算机交互就能通过网络传输数据。

**了解你的客户(KYC)**：银行或其他机构验证客户身份的过程，通常与监管或其他业务政策要求相关。

**移动网络运营商**：提供移动电话和数据服务的组织。

**美国国家标准与技术研究所**：美国国家标准机构。

**需求方**：利用数字身份为用户提供有数字体现的应用服务的组织（例如零售银行、线上药店或航空公司）。

**信任提供商**：指导直接用户注册数字身份，并管理数字身份和数字交互生命周期的组织。

**万维网联盟**：一个由成员组织、全职员工和公众共同制定网络标准的国际社区联盟。

# 参考文献


1.《你可以信任谁？》，蕾切尔·博茨曼（Rachel Botsman），2017年，Portfolio Penguin
2.《下一个倒下的多米诺骨牌：在线服务用户密码的实证分析》，弗吉尼亚理工大学，2018年
3.《物联网：消费、工业和公共服务2018 - 2023》，Juniper Research, 2018年
4.《发展的认同，非洲商业计划》，世界银行集团，2018年
5. 制定联合国可持续发展目标16.9是为了到2030年为所有人提供合法身份
6.《2018身份欺诈：欺诈进入复杂的新时代》，Javelin Strategy & Research, 2018年
7.《美国更好的身份：政策制定者的蓝图》，Better Identity Coalition，2018年
8. 数据泄露水平指数，金雅拓公司（Gemalto），2018年
9. 综合身份欺诈工作组，Auriemma Group，2017年
10.《数字身份的未来：全球专家洞见》，与万事达合作的未来议程，2019年
11. 万事达卡，2017年1月至11月
12.《数字身份的蓝图》，世界经济论坛，2016年