# 构建数字信任体系，助力数字经济发展

BJCA
数字认证

北京数字认证　詹榜华

2021年5月

# 目录

# 信任是社会秩序的基石

“信任是社会生活的基础、是简化复杂的机制之一、是经济交换的润滑剂、是一种社会资本，只有高度信任的社会才能构筑稳定、规模庞大的商业组织以应对全球经济的激烈竞争。”

——弗朗西斯·福山：《信任》

**信任是网络秩序的基石，是数字交互的基础和前提，没有信任的数字世界难以运转**

# 数字信任的定义

- **网络信任体系**是以密码技术为基础，以法律法规、技术标准和基础设施为主要内容，以解决网络应用中身份认证、授权管理和责任认定等为目的的完整体系（中办发【2003】27号文、国办发【2006】11号文）

- **ISO/IEC 25010:2011**标准体系中，信任是：
  - **用户或者其他相关人员对产品或系统能否按照预期正常执行的信心程度**

- **Gartner将“数字信任（Digital Trust）”定义为：一种可以衡量的信心，包括四个方面，具有十个评价指标：**
  - 个人、企业、业务或其他实体就是其本身，或者与它们所声称的身份一致；
  - 它们可以代表自己，也可以由另一个实体忠实地代表；
  - 它们在数字世界互动中能够充分表达自己的意愿；
  - 它们以真实、可预测、可靠、安全、合规、符合道德、尊重隐私的方式行动。

# 各行各业的价值潜力，来自于数字信任的驱动

**10%** 的信任提升带来 **36%** 的经济效益提升

信任技术 ＋ 应用场景 ＝ 价值创新

数字证书　多方计算
电子签名　零信任
区块链　密码云服务
同态加密

电子合同　电子处方
电子证照
电子档案　电子发票
电子工单
电子存证

# 数字身份管理+政府服务：为互联网+政务服务提供信任

**身份服务提供商**

- **政府**
  身份证、电子执照...
- **第三方CA**
  数字证书...
- **运营商**
  手机号...
- **社交网络**
  微信、支付宝...

**身份认证网络及生态系统**

**业务应用（身份认证依赖方）**


- 实名为核心的全省统一认证
- 规模化实名认证（数千万公众、数百万法人、数十万政府工作人员）
- 多种身份核实渠道、多种认证凭证
- 移动电子印章
- 跨系统互认机制
- 支持数千万用户高频访问

# 电子签名+证照：为各行业数字化提供可信凭证

## 电子签名为各行各业各种证照、凭证电子化过程中提供信任


- 电子成绩单（清华、北大...）
- 航空维修电子工单（国航、东航...）
- 密码产品型号证书（国密局）
- 发明专利证书（知识产权局）
- 出入境记录电子查询凭证（移民局）
- 国外学历学位电子认证书（教育部）
- 海关专用电子缴纳书（海关总署）
- 电子残疾人证（残联）
- 非税票据（财政部）
- ...

# 电子合同+企业供应链：为企业数字化转型建立交易信任

## 具有法律效力的数字化交付，革命性的改变交易模式


**传统纸质合同盖章流程：七步**

乙方盖章 → 快递给甲方 → 甲方审核校对 → 甲方盖章 → 快递回乙方 → 填写交接单 → 逐页扫描归档

**全流程电子化合同盖章：一步**

合同统一发送至电子合同平台，合同相关方在线预览并完成电子盖章，签署后合同自动归档

**签订周期平均缩短90%　合同费用平均下降70%**

vanke 万科

### 商业机会

突破传统商业的时空束缚，创造跨区域、全天候交易、缔约的可能，为企业拓展商业机会

### 业务效率

数字化协同处理，省略流程等待、寄送、校对、的过程，提升企业效率

### 安全管控

可靠签章技术，杜绝“萝卜章”风险；数字化安全加密保管，避免错配、丢失、外泄等问题

### 节约成本

电子合同免除了纸质合同的高额的耗材、仓储、快递成本，节省管理纸质成本的专人人力成本

# 数字证书+车联网：建立数字身份的信心

**信任主体海量化、泛在化，信任建立实时性、匿名性、随遇接入能力**

- 车联网环境下，高速行驶的汽车必须快速完成与各类实体的认证，对证书编码格式、传输带宽、交互时延都提出了极高要求
- 既要在关键时刻证明身份，又要在平时保护隐私的情况


# 目录

# 网络社会信任的新特征

传统社会中单纯依靠法理、契约等，建立在交互双方或有限实体之间的“信任”发生了新变化。

## 信任关系的复杂

- 信任主体种类多，数量大，企业、个人、算法、数据、设备等..
- 不同网域间彼此互联，实体互不相识


## 信任周期的短暂

- 网络空间充斥威胁，信任程度动态变化
- 已有信任可能瞬间瓦解


## 信任的可传递

- 信任的担保方不再仅限于个人或企业
- 软件接口、设备和第三方服务等各种无行为能力的实体开始充当信任传递的代理

# 构建数字信任体系的挑战

## 跨域互信

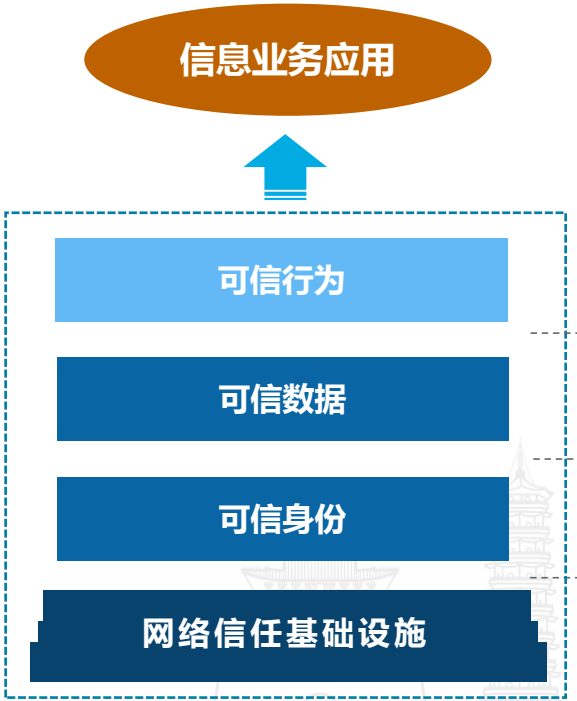
网络实体和信任关系的指数级、规模化增长，使得各类主体之间的跨域互信变得愈发困难

## 信任度评估

在充满不确定性的网络空间中，需要对行为体进行持续化、动态化、细粒度的可信衡量和监管

## 隐私保护

# 网络信任体系的分层与扩展




**可靠的技术手段+完善的监管措施**

个人、设备、企业、产品/服务等按照预期正常执行

数字签名、移动设备管理（DMD）、检测/认证/监测和追溯..

实现数据的机密性、完整性、可用性等信任要素和属性

数据脱敏、电子保全、容灾备份..

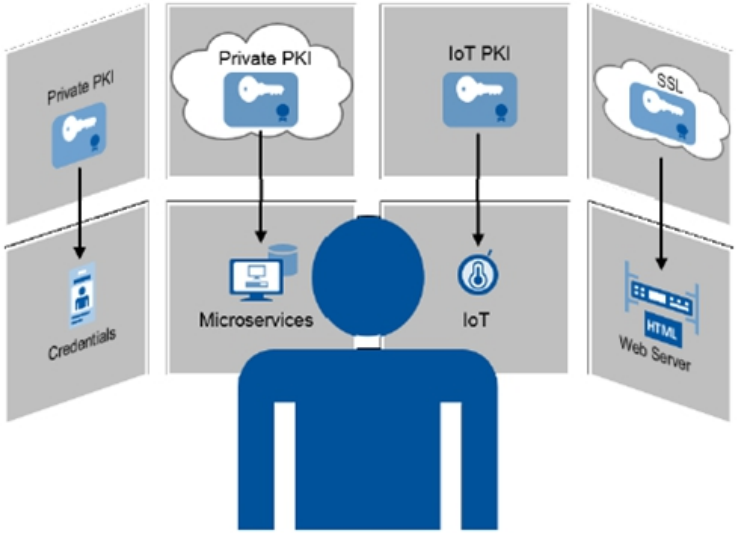
数字身份的唯一标识、真实身份的在线核验和鉴别...

OTP、生物特征、数字证书..

网络实体间建立安全可靠信任关系的根基

PKI、PMI、KMI..

# 基础设施：信任基础设施从外置走向内生




- 适配云、物联网、移动互联等的**内生信任基础设施**成为新的发展方向，信任基础设施本身可作为可信服务提供

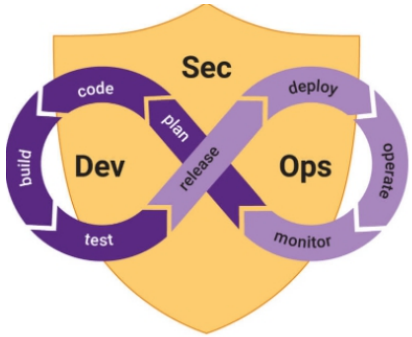
- **云密码基础设施**兴起，与传统信任基础设施（如PKI、PMI、KM等）融为统一信任基础设施的一部分

# 身份可信：静态单一的边界信任走向技术多元化的动态信任


- 身份的可信不再依赖传统内网边界
- 认证和授权逐渐从静态走向动态
- 信任需基于网络威胁状态和业务资源价值实时评估和调整

网络应用呼唤兼顾**生物特征认证**灵活便捷和**强隐私保护诉求**的身份可信技术

# 数据可信：从安全传输和存储拓展到安全计算




## 数据安全隔离

通过计算机系统中内生的密码能力，构建相互隔离的机密计算空间；

以保证云计算环境下多租户场景的数据隔离，包括Intel SGX、AMD SEV以及Arm TrustZone等技术。

## 可信计算环境

传统的数据可信重点关注点到点安全传输，未来逐步拓展到数据使用过程的安全可信；

例如用以解决软件供应链安全的代码签名、DevOpsSec等技术。

**In use**

Protect/Encrypt data that is in use, while in RAM and during computation.

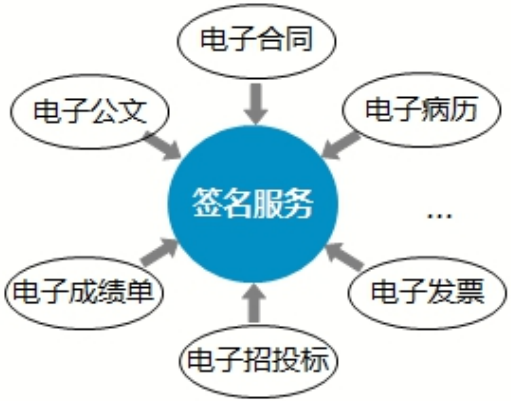
CONFIDENTIAL COMPUTING CONSORTIUM

## 安全外包计算

同态密码和安全多方计算是外包计算场景下用以保护用户数据隐私的有力武器；

支持在数据计算过程中不泄露给外包方，例如 IBM HELib和微软seal等同态加密技术。

# 行为可信：多种技术机制保证意愿表达和可信追溯




以**电子签名**为核心的可信服务，成为保证业务过程合规、行为意愿表达的主要手段，如电子合同、电子病历、电子发票等


借助**区块链技术**，可形成适用于泛中心化场景下的网络信任机制，能够在跨越各种异构系统和体系的情况下构建以技术为背书的分布式信任

借助**人工智能和机器学习**，能够有效对业务行为数据进行分析和画像；其结果可用于各类网络实体行为追溯和责任认定，作为实体间建立信任的依据

# 建设可度量的数字信任体系

## 顶层设计

研究多层次、多维度、可度量的数字信任标准体系，明确信任度量总体要求和基础设施参考模型，促进不同行业领域中信任基础设施的互信互认

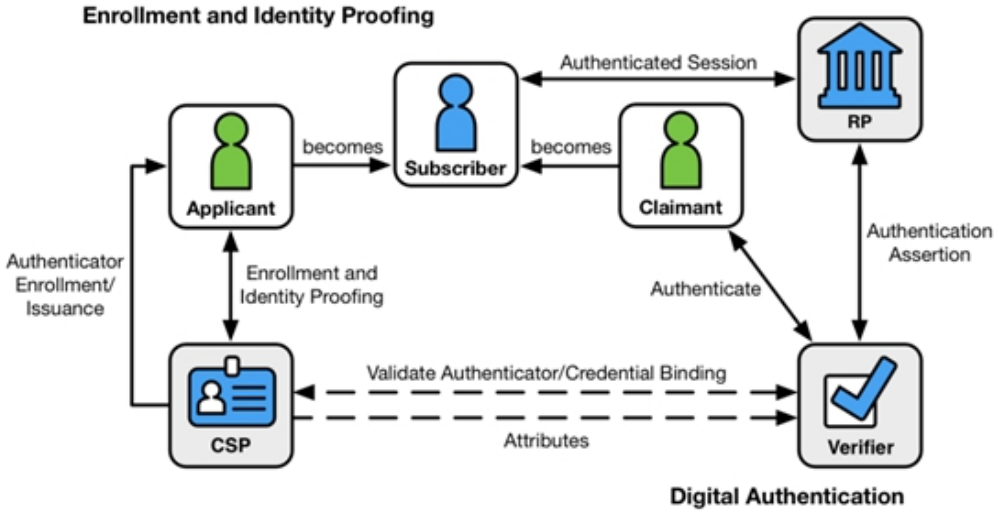
## 度量手段

研究细粒度、动态信任评估技术手段，逐步完善信任度量相关的技术、产品、服务、检测标准，优选典型行业和应用场景推动信任评估新技术的落地应用

## 管理监管

研究信任体系参与方关联关系和监督管理模型，编制信任监管、追溯、取证机制的相关标准规范，构建以信任度量手段为支撑的监管体系

# 美国：实施网络空间可信身份战略并初见成效



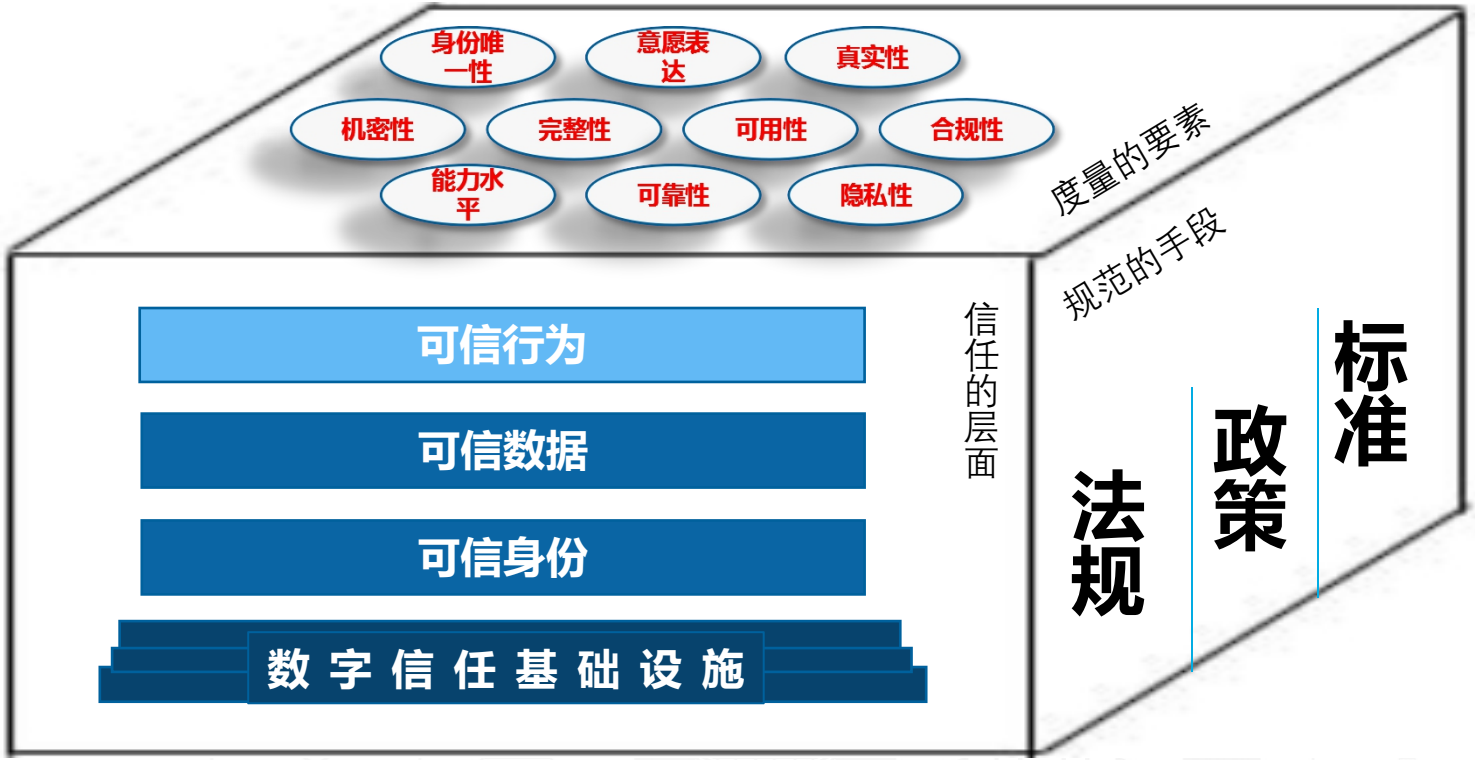

- NIST建立**数字身份标准框架**，将识别数字身份的过程分为**身份核实、身份鉴别和身份联合**三个环节，明确各环节安全保障级别
- NSTIC**开展引导工程实践**，通过4批共22个试点项目来调动参与各方积极性，范围涵盖医疗保健、金融、教育、零售、航空航天和政府部门等多个领域

# 欧盟：注重从监管层面增强成员国之间的互认互信

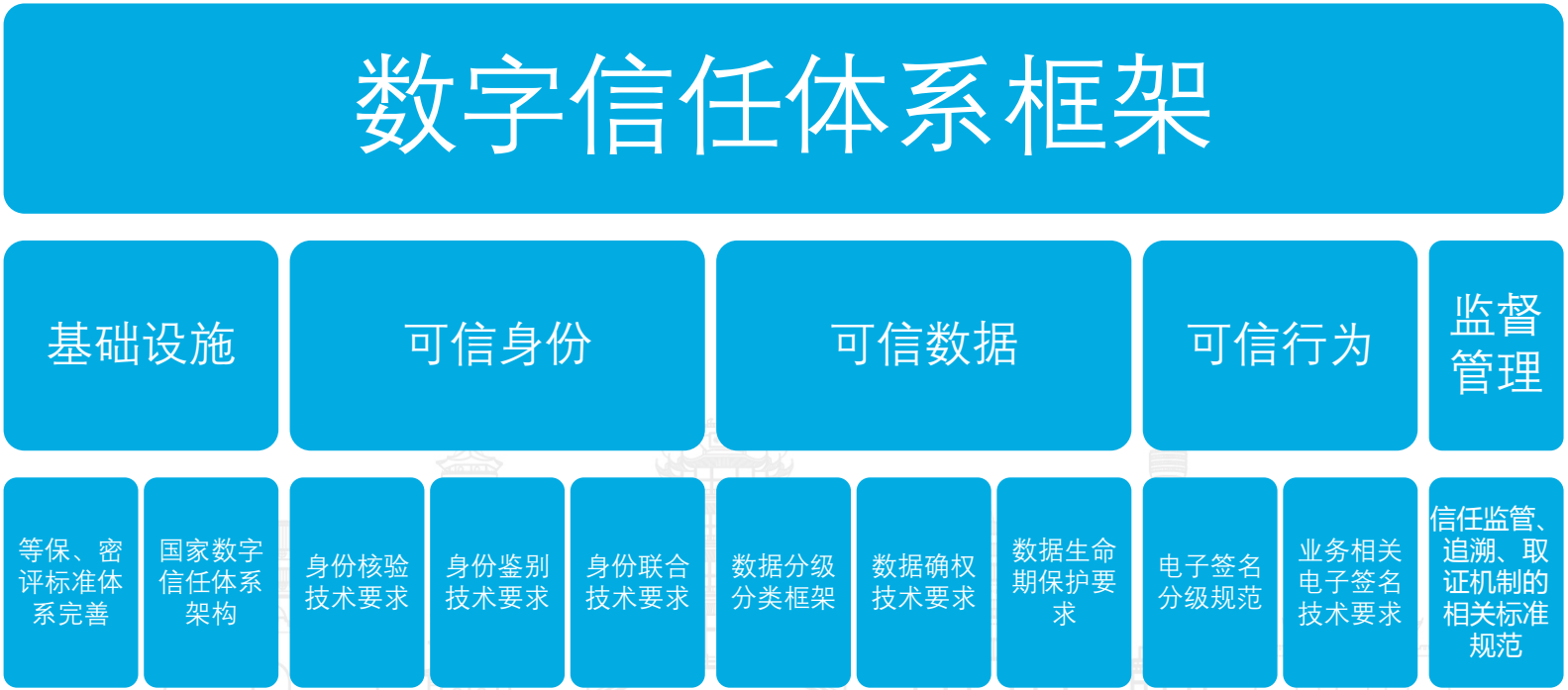
- 借助国际CAB联盟（CA/Browser Forum）的**审计评估机制**对合格信任服务提供方及其服务开展周期测评和抽查监测
- 以签发**信任列表**（ Trust lists ）和**可信标识**的方式规范可信服务（Trust Services）监管
- 通过**电子身份证（eID）**实现身份互认和跨境数据交互（如远程医疗记录调取、移民手续办理、在线招投标等）

**29个成员国家/地区，202个有效的信任服务提供者纳入监管，搭建网络信任顶层指导框架（信任金字塔模型）。**

# 数字信任体系：统一管理和技术框架下的分层可度量信任



# 标准化工作建议


数字信任体系框架
基础设施
可信身份
可信数据
可信行为
监督管理
等保、密评标准体系完善
国家数字信任体系架构
身份核验技术要求
身份鉴别技术要求
身份联合技术要求
数据分级分类框架
数据确权技术要求
数据生命期保护要求
电子签名分级规范
业务相关电子签名技术要求
信任监管、追溯、取证机制的相关标准规范

全国信息安全标准化技术委员会
2021年第一次工作组“会议周”活动