# 关于数据二十条

首次提出了可信流通这个说法。

关键概念：数据可信流通体系

会在以后的数据流通中发挥作用

鼓励探索相关技术、标准、方案

# 关于可信

## 相关背景

可信提出的背景：数据流通中的不可信风险

数据有持有权、加工使用权、经营权。存在越权使用、持有权保障确实的问题

数据要素离开持有方后，持有方还有管控需求和责任

信任的四个要素、离开持有方安全域后的破坏情况、可信流通如何保障信任

|  |  |  |
| --- | --- | --- |
| 要素要求 | 破坏原因 | 可信流通 |
| 身份可确认  （是谁） | 主体不清 | 身份可以明确 |
| 利益可依赖  （委托利益） | 利益诉求不一致  （拷贝和滥用） | 利益可以对齐 |
| 能力有预期 | 能力水平不一样  （无法做好保障） | 能够有效度量能力 |
| 行为有结果 | 责任链路难追溯 | 责任明晰，可以追溯 |

## 相关技术

### 可信数字应用身份

CA证书相关技术的局限性：只认证了主体和个人，没有认证数字应用实体

替代技术：可信计算技术，基于可信硬件芯片这种纯技术手段，验证某个节点的软件和硬件

从主体身份扩展到应用身份

### 利益对齐的核心：使用权跨域管控

明文计算的问题：数据持有权和使用权捆绑，容易拷贝、泄露

使用权跨域管控的两个层面：

1、数据持有者能对数据的进一步使用进行决策（利益对齐）

(1)限制运维人员

(2)管控研发流程

(3)全链路审计保障

2、规范化的技术体系支持

通过隐私计算、可信计算、机密计算等技术路线实现

满足跨域管控要求

### 能力预期

不可能三角：

安全要求

功能复杂度

单位成本

通用安全分级：1-5级，从低到高分别是

|  |  |
| --- | --- |
| 基础防护 | 基于主题信任的权限管控（传统数据沙箱） |
| 中等防护 | 密态管道模式（FL）、密态枢纽模式（TEE） |
| 安全设计 |
| 攻防检验 | MPC、TECC |
| 安全证明 | FHE |

单位成本的计量单位是：明文分布式计算的成本

### 全链路审计

控制层面：可信计算和区块链（跨域管控 + 全链路审计）

数据层面：隐私计算（密态枢纽 + 密态管道）

密态数据流转的损失比较小，追溯成本更低

## 技术信任保障可信流通

数据密态，可以做到数据存储、计算、运维、研发、交付、销毁全链路安全可控

数据可信流通背后的基础设施：密态天空计算

这是跨云的基础计算设施

覆盖数据流通的全部链路