HNSF
Health Network Security Forum 2017
医疗网络安全论坛

互联网医疗服务信息安全新技术探究

国家信息安全工程技术研究中心

李增欣

2019年4月28日

目录

互联网+“医疗健康”发展的背景

互联网医疗面临的信息安全问题

互联网医疗服务信息安全新技术

互联网医疗发展的背景

政策背景

HNSF Health Network Security Forum 2017 医疗网络安全论坛

国务院办公厅《关于印发全国医疗卫生服务体系规划纲要(2015-2020年)的通知》

国务院办公厅《关于促进“互联网+医疗健康”发展的意见》

健康中国规划纲要“三个一”工程

关于加快推进人口健康信息化建设的指导意见

《关于印发全国新型农村合作医疗异地就医联网结报实施方案的通知》

《国务院关于促进信息消费扩大内需的若干意见》

《居民健康卡应用目录》

12部委《关于加快实施信息惠民工程有关工作的通知》

《省级统筹区域人口健康信息平台应用功能指引》

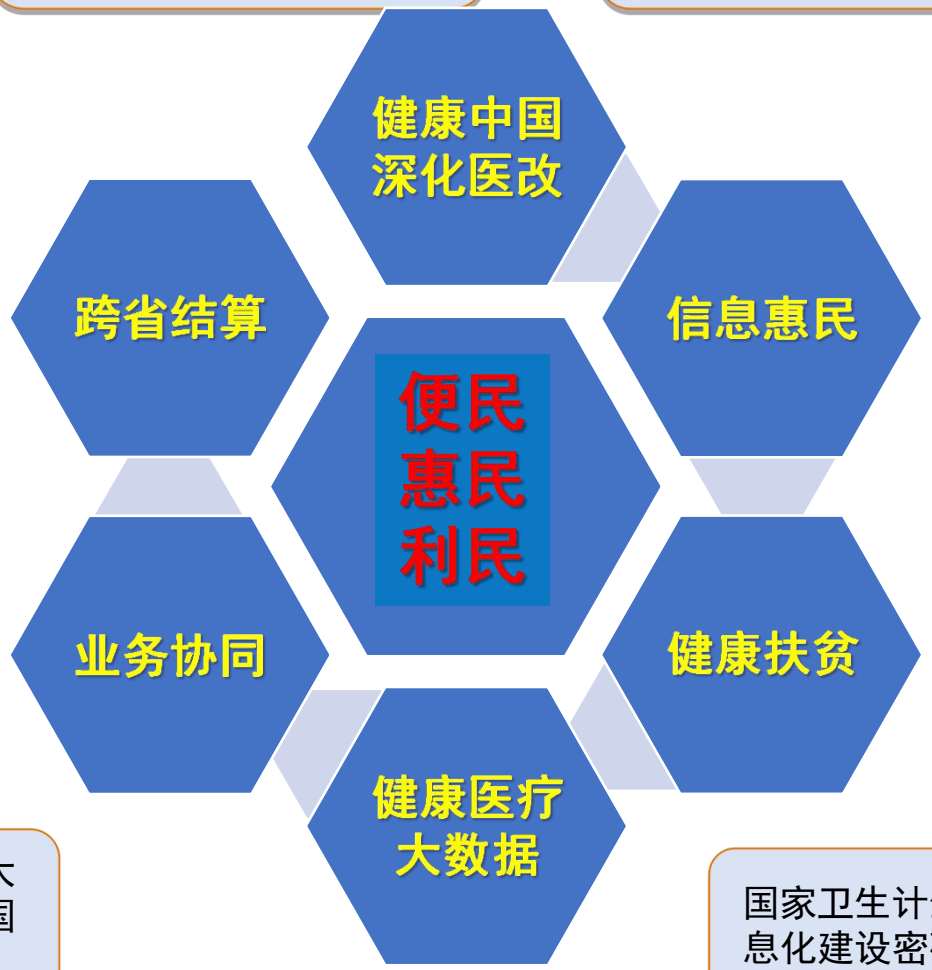
《中共中央　国务院关于打赢脱贫攻坚战的决定》

《医院信息平台应用功能指引》

15部委《关于实施健康扶贫工程的指导意见》

《关于促进和规范健康医疗大数据应用发展的指导意见》国务院办公厅

国家卫生计生委关于卫生计生行业信息化建设密码应用的规划和实施意见



互联网医疗发展的背景

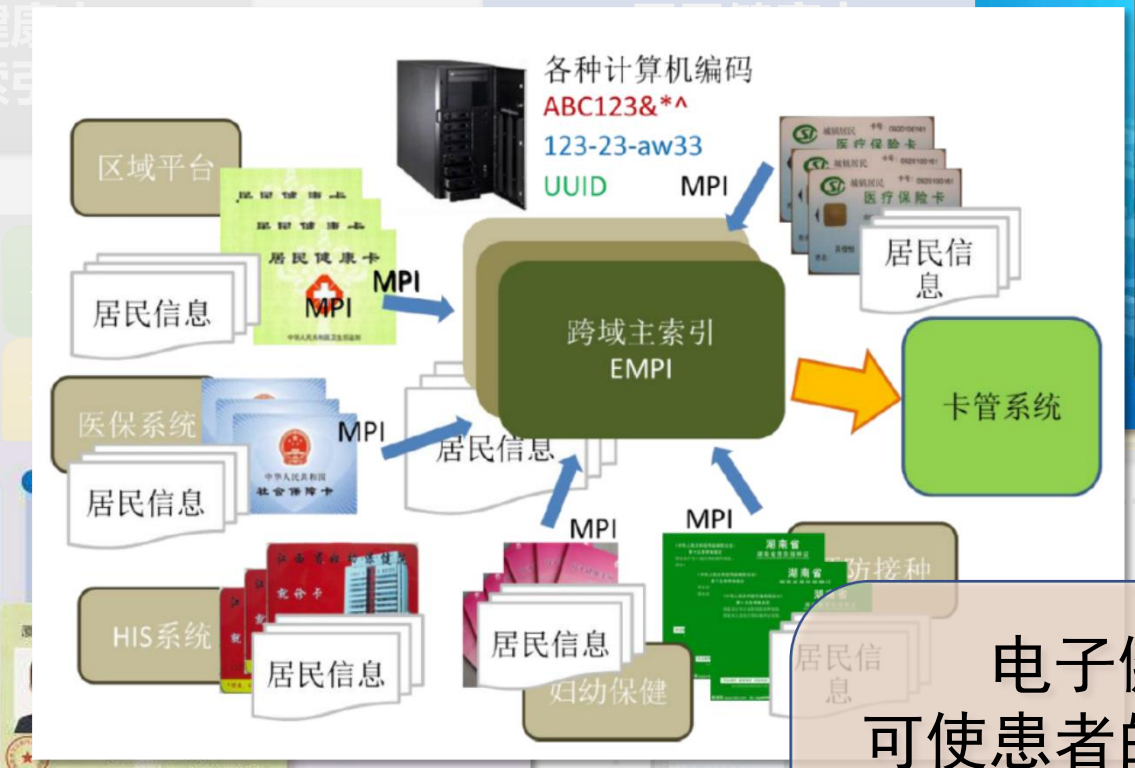
“三个一”工程：到2020年力争实现：

- 每个家庭拥有**一名合格的家庭医生**
- 每个居民拥有**一份伴随一生的居民健康档案**
- 每个居民拥有**一张功能齐备的居民健康卡**

实现人人享有基本医疗卫生服务。

“三个一”工程纳入《健康中国2030规划纲要》

电子健康卡



电子健康卡的发行与应用
可使患者的就医方式发生根本改变

从线下到线上

线下线上融合

互联网医疗发展的背景

从线下走向线上

HNSF Health Network Security Forum 2017 医疗网络安全论坛

手段 “三个一”工程、“新三一”规划

技术 大数据、云计算、人工智能、智能设备

渠道 互联网、移动互联网、物联网、有线电视

便民
惠民
利民

互联网医疗面临的信息安全问题

新的变化

HNSF Health Network Security Forum 2017 医疗网络安全论坛

新的挑战

场景变化

- ✓ 从封闭独立体系，自我相对完备的安全机制
- ✓ 到区域医疗协同，医疗机构互联涉及医务人员的安全认证、授权访问
- ✓ 到互联网医疗，患者的身份认证，个人隐私数据保护，医疗大数据安全等

范围变化

- ✓ 从医院内部（院内）->
- ✓ 医疗机构之间 ->
- ✓ 区域医疗平台 ->
- ✓ 互联网（院外）

对象变化

x2

- ✓ 医疗机构
- ✓ 医务人员
- ✓ 普通患者
- ✓ 药店
- ✓ 第三方服务机构
- ✓ 支付机构

院内简单 院外复杂

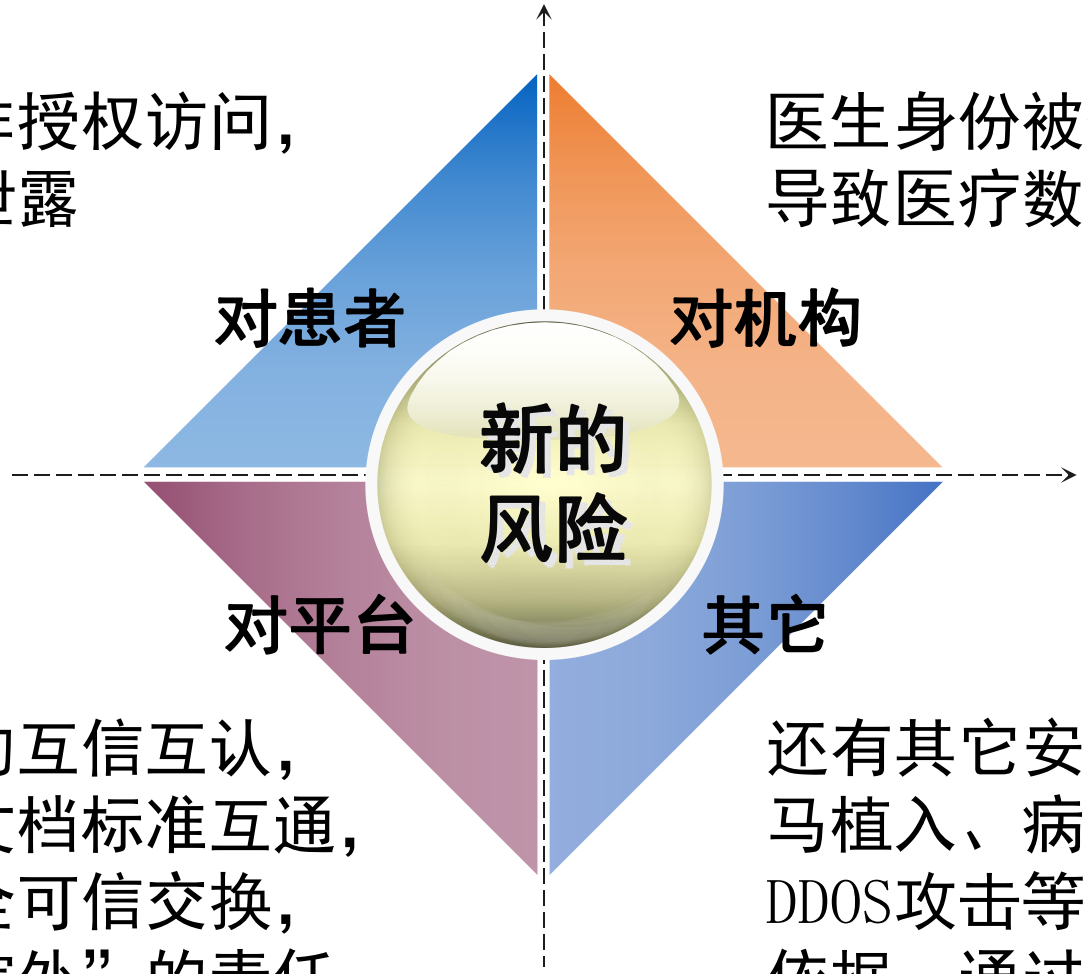
院内的安全风险已由院内的安全防护体系得到有效控制，但院外需要新的手段

互联网医疗面临的信息安全问题

安全风险

身份被假冒、非授权访问，
导致个人隐私泄露

医生身份被假冒、非授权访问，
导致医疗数据被窃取、被篡改



跨区域跨机构的互信互认，
不同机构医学文档标准互通，
在线、离线安全可信交换，
“院内”与“院外”的责任
隔离与认定

还有其它安全风险，比如：木
马植入、病毒入侵、网页篡改、
DDOS攻击等。这需要以等保为
依据，通过网络安全防护设备
或系统的配置和部署来规避

互联网医疗面临的信息安全问题

跨域认证

医生、患者“院内”及跨院可信身份认证

隐私保护

患者个人隐私数据保护及数据脱敏，以及大数据传输存储安全

数据可信交换

医疗数据的一致性完整性和防篡改，跨院跨域的在线离线可信交换

行为追溯

跨域医疗行为的监管与追溯、责任划分与责任认定

以国产密码为核心解决互联网医疗面临的信息安全问题

打破惯性思维，采用新技术、新方法、新手段解决互联网医疗安全需求

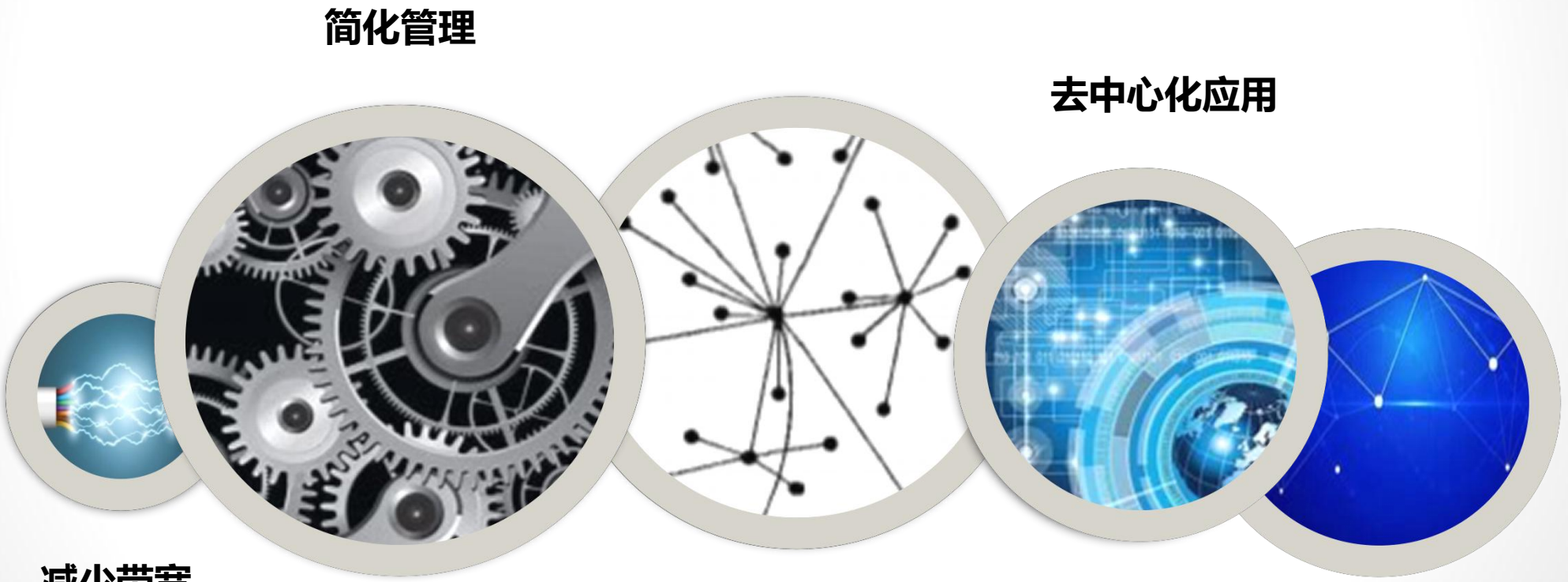
采用基于标识的无证书认证技术实现跨院跨域的身份认证	采用国产安全二维码技术实现跨院跨域数据离线可信交换	采用安全网关与赋码技术实现跨院跨域医学文档标准转换	建设溯源平台对医疗行为过程进行追踪溯源提供监管手段	利用国产SSLVPN及IPSECVPN技术保护数据链路安全

以电子健康卡为切入点，做到线上线下一体化

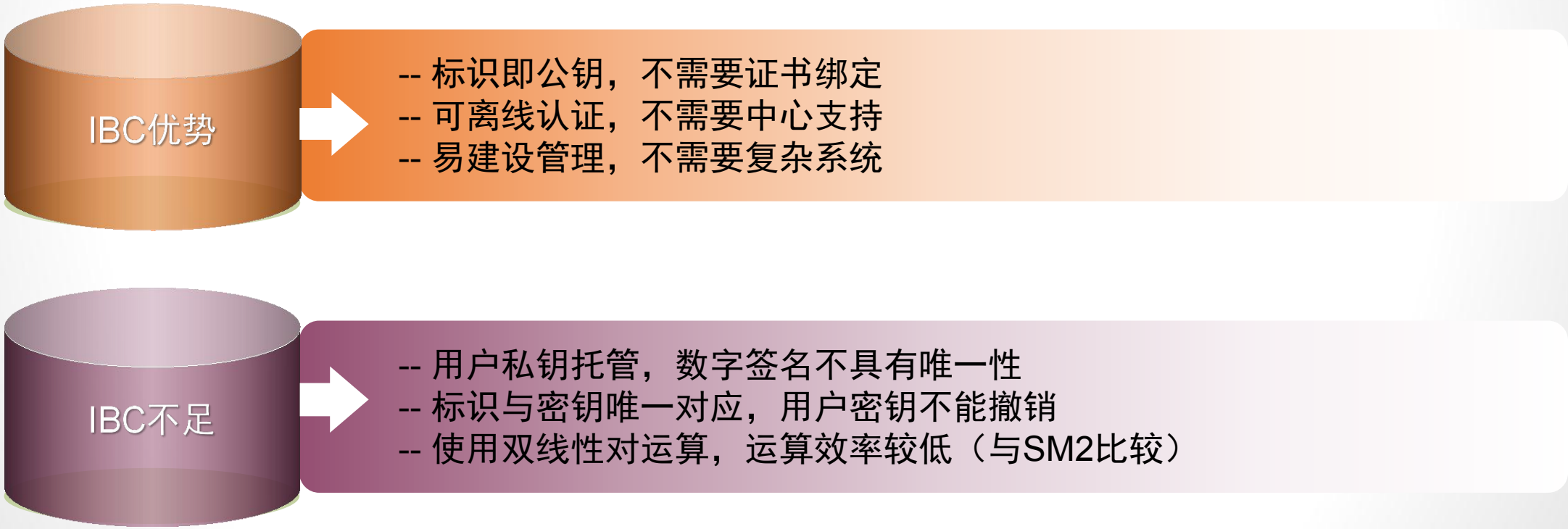
互联网医疗信息安全新技术

新技术优势

随着物联网、移动互联网的快速发展，在新业态下PKI/CA的适应性已经显现出它一定的局限性。新的业态对公钥密码体制提出了新的需求：



近年来，国内外密码专家都在致力于研究新的公钥密码体制，其核心是如何解决公钥认证问题，目前最具代表性的就是**标识认证技术**。国密局2016年3月28日发布了SM9算法，为IBC的发展提供了核心算法支撑。



CLA的技术定位和技术路线

- 采用标识认证技术，去中心化，支持离线认证
- 不使用数字证书，减轻证书管理的负担
- 用户私钥只有自己掌握，数字签名具有唯一性
- 支持密钥撤消，可再生成新的密钥对
- 不用双线性对运算，提高计算效率
- 融合自证公钥密码体制和无证书公钥密码体制
- 借鉴PKI/CA系统的管理体系架构
- 采用现有SM2椭圆曲线密码算法
- 兼具PKI/CA、IBC的优点

标识认证与证书认证的差异

PKI/CA – 公钥基础设施/证书认证体制
IBC – 基于标识认证体制
CLA – 基于标识的无证书认证体制
CPK – 组合公钥认证体制
CFL – （密码专家姓氏所写）
IKI – 标识密钥基础设施

基于证书的公钥密码体制：CA
基于标识的证书认证体制：CFL、IKI
基于标识的公钥密码体制：IBC、CPK、CLA

CLA是PKI/CA、IBC技术优势的有机融合

参数指标	PKI/CA	CLA	IBC
双线性对运算	不使用	不使用	使用
使用证书	用	不用	不用
双密钥支持	支持	支持	不支持
建设管理复杂度	复杂	简单	简单
运行效率	一般	高	低
资源占用	多	少	少
密钥撤销	可撤销	可撤销	不可撤销
基于标识的签名（IBS）	不支持	支持	支持
基于标识的认证（IBI）	不支持	支持	支持
基于标识的密钥协商（IBAKE）	不支持	支持	支持
基于标识的公钥加密（IBE）	不支持	不支持	支持
密码设备	现有	现有	新研制
管理中心依赖度	高	较低	低

传统的身份认证：

方便的不安全

危

用户名　口令　SMS　OTP

- 拖库、破解
- 密码复杂度要求
- 密码更换频率要求
- 密码非重复设置要求
- 短信劫持
- 伪基站
- 钓鱼网站

安全的不好用

难

U盾　蓝牙盾　SD盾　音频盾

- 需要随身携带外置设备
- 移动场景不符合用户的使用习惯
- 难以推广
- 成本高

安全可靠、体验好的产品在哪里？

手机即是令牌

手机是人身体的一部分
一切控制的中心

不需要额外介质

无需硬件介质
投入低，体验好

安全性媲美U盾

安全
合规

手机变U盾，安全随身行

身份认证

“云+端”硬件级加密安全保护专利算法确保身份安全

“一刷一扫”轻松实现手机、PC统一身份登录认证

电子签名

支持实名认证，移动互联网时代U盾的最佳替代方案

支持生物识别、设备指纹、口令等多因素认证模式

安全机制和原理

支持指纹、人脸等主流生物特征识别

移动端采取了防逆向、防篡改、防调试、防窃取等多种措施，防止恶意程序或攻击者绕过用户身份认证机制

支持国多种数字认证技术，合法合规

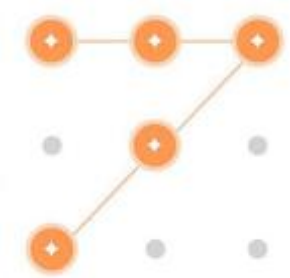
手机硬件信息参与密钥计算，复制到其他手机无法解密

多因素认证

指纹

人脸

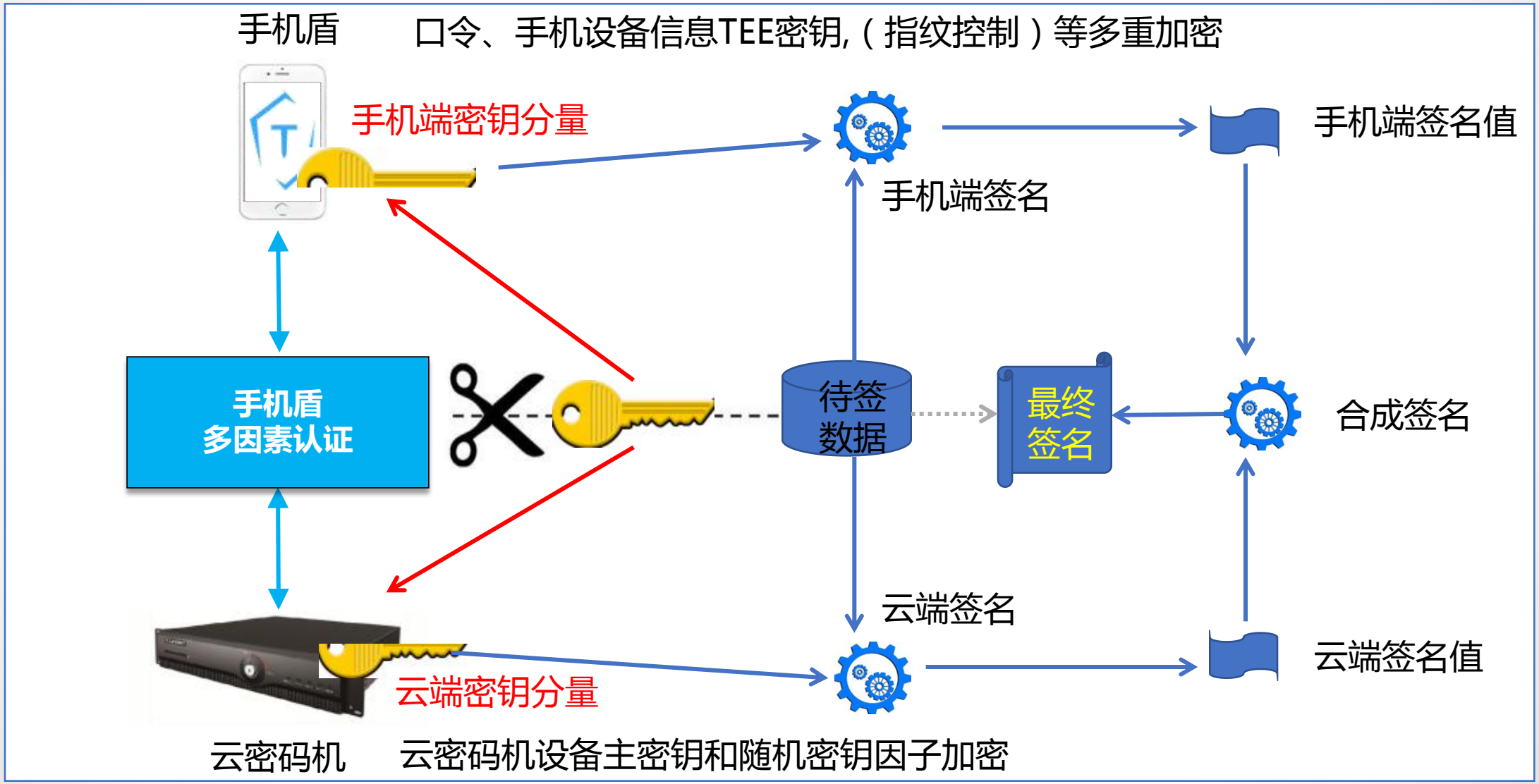
口令



手势密码

设备指纹

密钥分隔与协同签名


手机盾
口令、手机设备信息TEE密钥,（指纹控制）等多重加密
手机端密钥分量
手机端签名
手机端签名值
手机盾
多因素认证
待签
数据
最终
签名
合成签名
云端签名
云端签名值
云端密钥分量
云密码机
云密码机设备主密钥和随机密钥因子加密

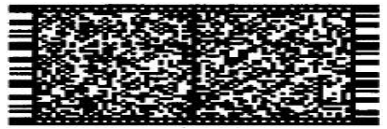
二维码概况

- 智能手机的大量普及使二维码应用有了爆炸式的增长。
- 二维码扫描认证、二维码扫描购物、二维码扫描查询、二维码扫描支付等，二维码应用已经融入到日常工作与生活的各各角落。
- 我国二维码标准共有6个，它们是QR码、PDF417码、GM码、CM码、汉信码、D9ing码。QR码是日本技术，PDF417码是美国技术，非自主知识产权，其它4个标准都具有国内自主知识产权。
- 目前，常用的二维码主要是QR码和PDF417码。

QR码,日本专利

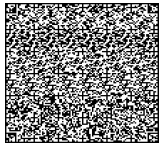
PDF417码,美国专利

GM网格矩阵码



CM紧密矩阵码

汉信码



D9ing码

二维码安全风险

- 二维码技术已经相对成熟，任何用户都可生成二维码，从外观不能判断其安全性。由于没有安全机制和监管措施，这就给黑客利用二维码作案提供了机会。
- 用户一旦扫描了嵌入病毒链接的二维码，其个人信息、银行账号、密码等就可能完全暴露在黑客面前，酿成的后果可想而知。
- 2014年3月14日，央行紧急叫停二维码支付。

- 近年来，一些有识之士致力于二维码安全的研究，有关二维码应用的安全技术日趋成熟，风险逐渐可控。
- 中国银联发布了二维码支付相关技术标准和业务规范，建立相关系统设备软件的检测认证体系。

- 央行重新开放了二维码支付许可。
- 支付宝、微信、银联支付广泛使用。

- 但风险依然存在…

安全二维码—鼎九码（D9ing）

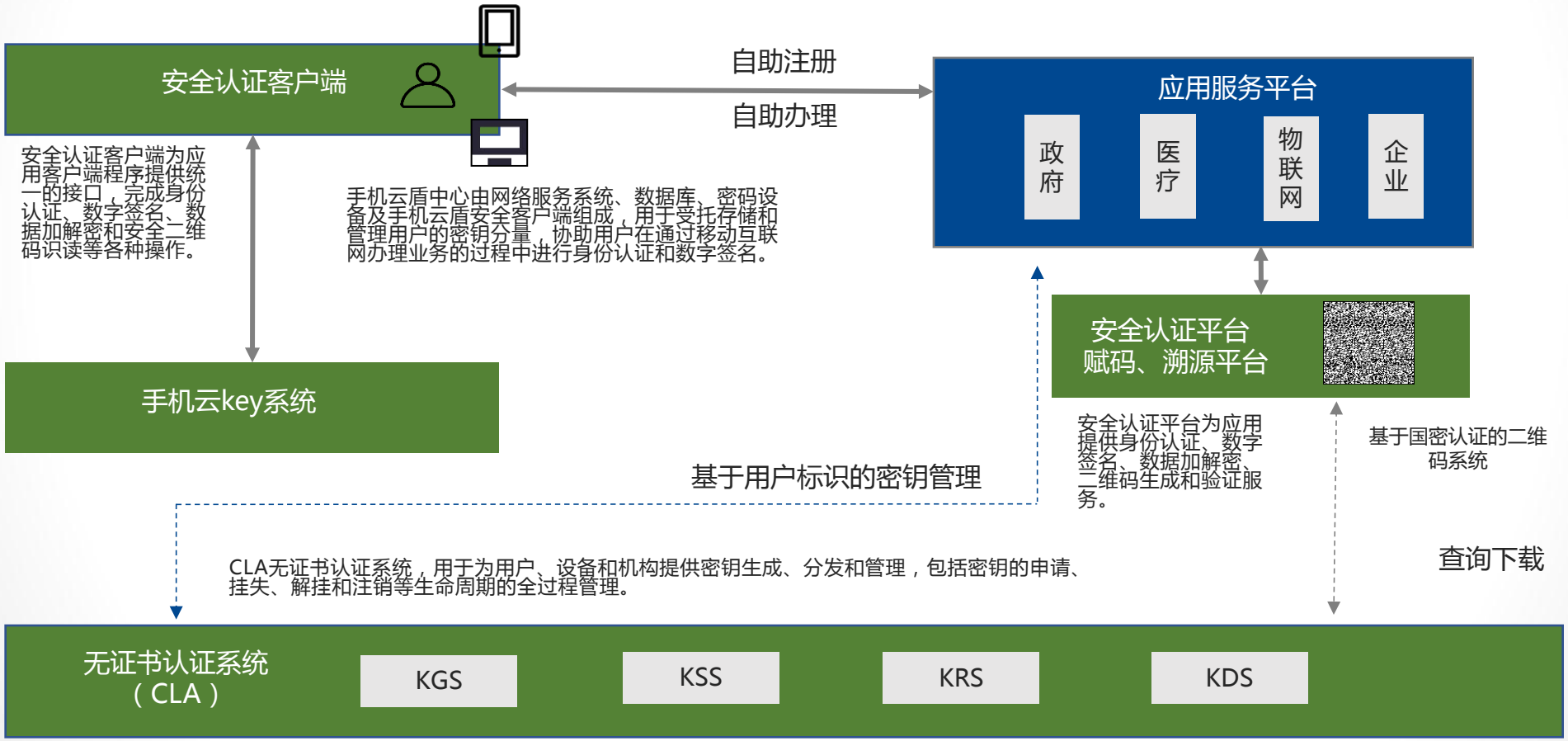
- 在二维码六国家标准中，目前只有鼎九码（D9ing）是安全二维码（防伪二维码）。
- D9ing码是在编码机制本身上实现其安全特性的，而不只是对内容加密。

- 主要特点：
  - 一物一码：所有的D9ing码都不同，即便内容相同
  - 一码一密：对编码信息及内容进行数字签名，防篡改
  - 生成可控：专用商用密码生成设备
  - 离线验证：在CLA的支撑下实现在线生成、离线验证

互联网医疗信息安全新技术

解决方案框架

CLA无证书认证系统、手机云盾系统、安全认证平台和安全认证客户端组成，与现有的应用服务平台中各业务系统对接构成统一的整体。

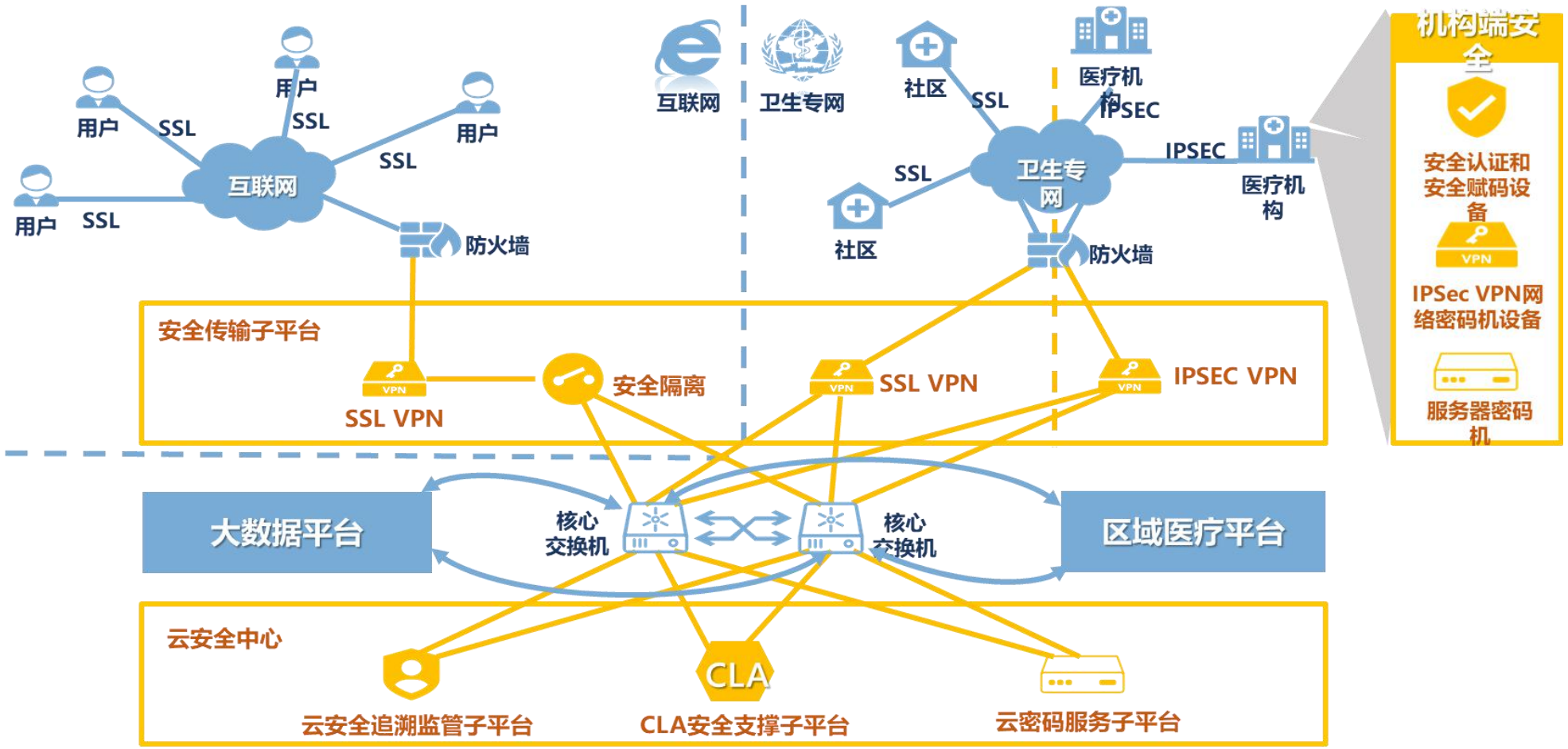


互联网医疗信息安全新技术

部署方式

互联网医疗信息安全新技术

网络拓扑



服务政府提高效率，服务市场优化资源，服务社会构建诚信

安全

CLA系统是安全基础设施

安全问题有保障了，万物互联能够提供更好、更快、更精准的服务，还能防止不法分子蓄意破坏、制造恐慌，譬如发送非法指令造成大面积停电、大面积停水、大面积停气等。

易用

物联网时代，万物互联

智慧城市、智能家电、智能终端、智能传感，可见智能世界已经来到我们面前。如何保证智能设备间的数据安全、指令权属？CLA是一种特别适合物联网的公钥密码体制，它集PKI/CA以及IBC优势，不使用证书符合窄带应用，可通过标识计算公钥展现标识密码的优势，公钥自证性保证终端身份的可靠，支持离线验证保证应用的活性。

发展

应用场景广阔

不仅可以给群众带来可信消息发布，还能实现产品追溯，为广大消费者带来利益。CLA的跨域认证、去中心化验证技术，应用范围广阔，不仅能实现国内互认，多国家多地区之间的互认也可简单实现，目前已在一带一路项目中应用，带来的影响正一步步扩大。

谢谢！