



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

强化安全创新 助力数字化转型

—— 在大规模分布式网络中应用密码技术的探索

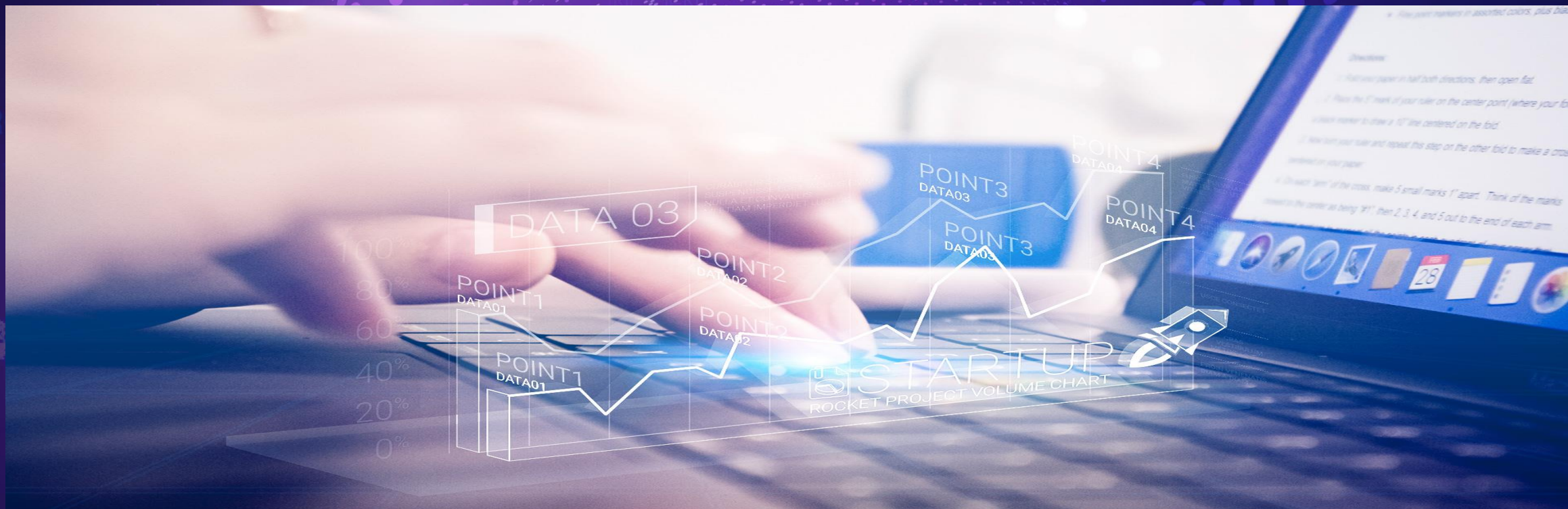


2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



关于飞天诚信





从支付到企业安全和万物互联，
飞天诚信的创新专注于数字安全的两个核心领域：身份安全和交易安全。



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

60,000,000+
产品年销量



10,000+
客户数量



1200+
全球专利



400+
研发团队



900+
全球雇员





2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



飞天诚信的担当： 应用自主可控密码技术保障网络空间安全



自主可控的密码技术是经过理论证明、可信的网络空间安全核心技术。目前，应用密码技术保障网络空间安全的顶层设计已逐步落地



2019年12月1日起
实施的网络安全等级保护系列标准
（“等保2.0”）中加入了密码技术的相关要求



《密码法》
2020年1月1日起实施



2020年5月9日，市场监管总局、国家密码管理局发布《商用密码产品认证规则》和《商用密码产品认证目录（第一批）》



国家互联网信息办公室、国家密码管理局等12个部门联合制定的《网络安全审查办法》自2020年6月1日起正式生效

架构不适配：典型的密码产品基于“信源-信道-信宿”模型，用于大规模分布式网络时显“重”，对网络性能影响比较明显；



接口不标准：大规模分布式网络协议栈和应用框架中缺少全局性、标准化的接口，应用密码技术、部署密码服务的工作量和复杂度有待优化；



产品可靠性待验证：密码应用一旦出现故障，将严重威胁网络可用性和系统业务连续性。大规模分布式网络对密码产品的可靠性要求极高，现有密码产品能否满足，有待验证。





突破瓶颈的思路：产学研用协同

01 鼓励、支持高校及科研院所研究论证适用于大规模分布式网络环境的密码应用基础模型



02 强化校企合作，及时将研究成果转化为新一代密码产品标准体系，设计研发新一代密码产品，推动标准尽快落地

03 依据新一代密码产品标准推动商用密码产品认证深化发展，鼓励应用单位使用经过商用密码产品认证的新一代密码产品





2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

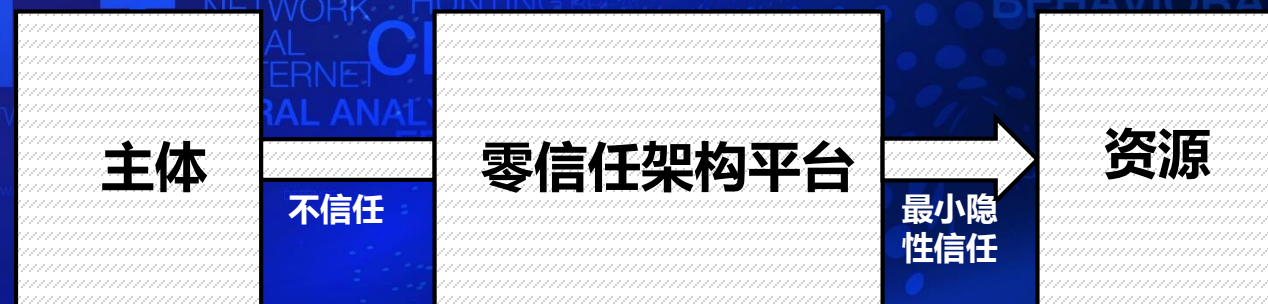


飞天诚信的技术尝试：基于零信任架构应用密码技术



“零信任架构平台是基于零信任架构构建的可运行的系统平台，零信任架构平台逻辑上位于主体和资源之间，对资源进行“隐藏”，确保默认情况下主体不具备对资源的任何访问权限。零信任架构平台提供身份识别、授权决策和信任等级评估等安全能力，针对主体对资源的所有访问请求，按照既定安全策略进行决策，决策通过后，可以赋予主体最小隐性信任，主体获得对资源的访问权限，否则访问请求被阻止或要求主体进一步证实其可信性”

——国家标准《信息安全技术 零信任参考体系架构》（草案）





访问令牌管理服务

分发和管理访问令牌，验证令牌的有效性

身份认证转接服务

与多种身份认证服务对接，向令牌管理服务提供标准化接口的身份认证服务

注册管理服务

应用使用飞天诚信统一认证平台所需的注册管理和配置

密钥管理服务

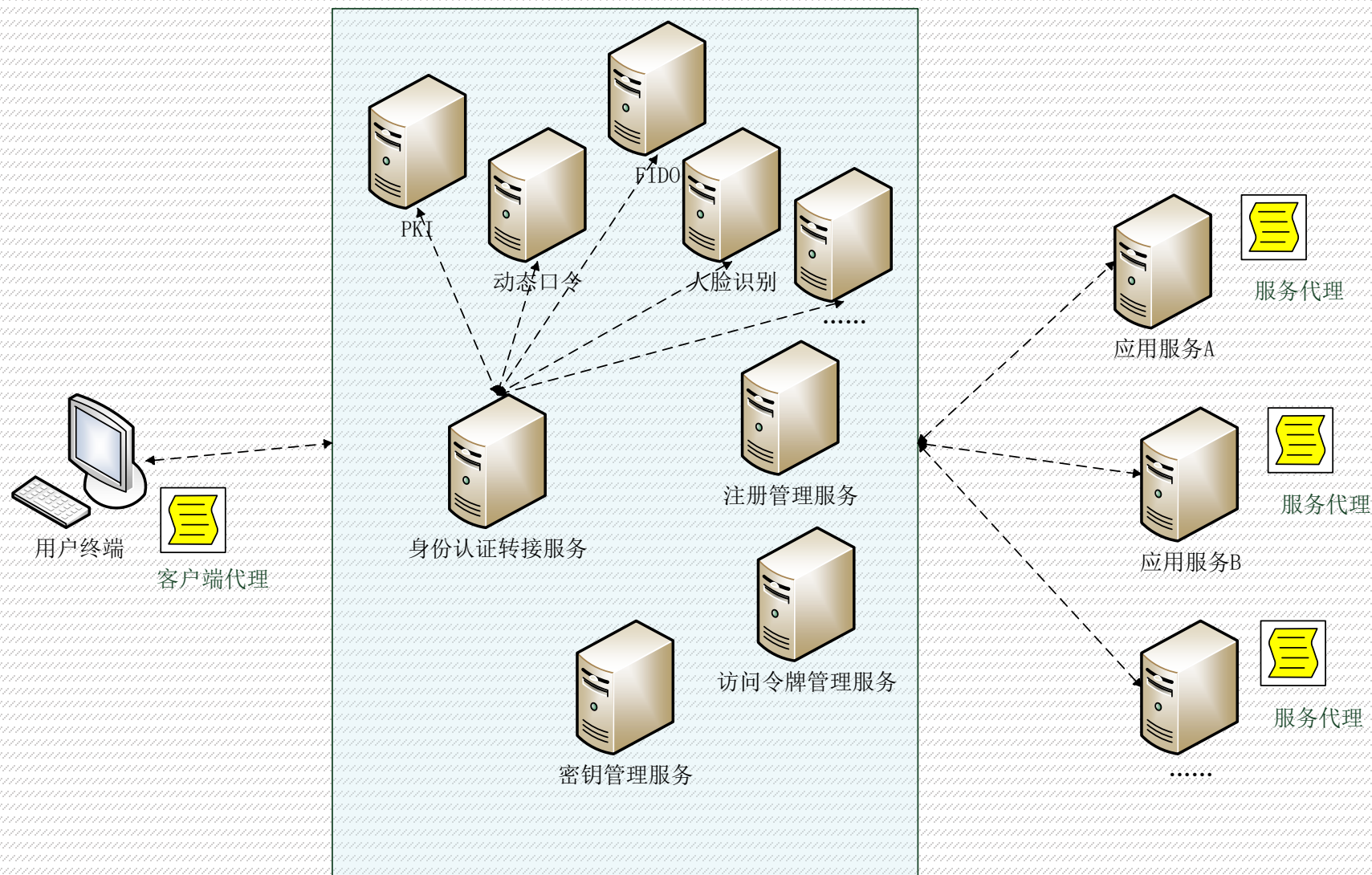
分发和管理会话密钥

身份认证服务

动态口令、数字签名、**FIDO**等多种可选，支持与第三方**CA**互连

客户端代理、服务代理

下载、保存和使用访问令牌及会话密钥



初步验证了零信任架构下应用密码技术的可行性

- 节点间的身份认证和数据交换使用自主可控的密码算法、密码协议等，符合国家密码管理部门要求
- 身份认证服务实现标准化接口，支持多种身份认证机制，可配置、可切换，接入平台的应用无需改动
- 密钥管理“中心化”与密码应用“去中心化”相结合，适应大规模分布式网络环境
- 应急预案有待验证



密钥管理“中心化”、
密钥使用“去中心化”



自主可控密码技术
应用



标准化接口



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



飞天诚信的产业生态尝试：数字身份产业联盟(DIDA)



分布式
身份信息可用于多个中心节点

可移植

由于身份控制权完全自主控制，使得身份拥有很高的可移植性。同一份身份信息，可以同时提交给多个验证机构，无需重复申请。

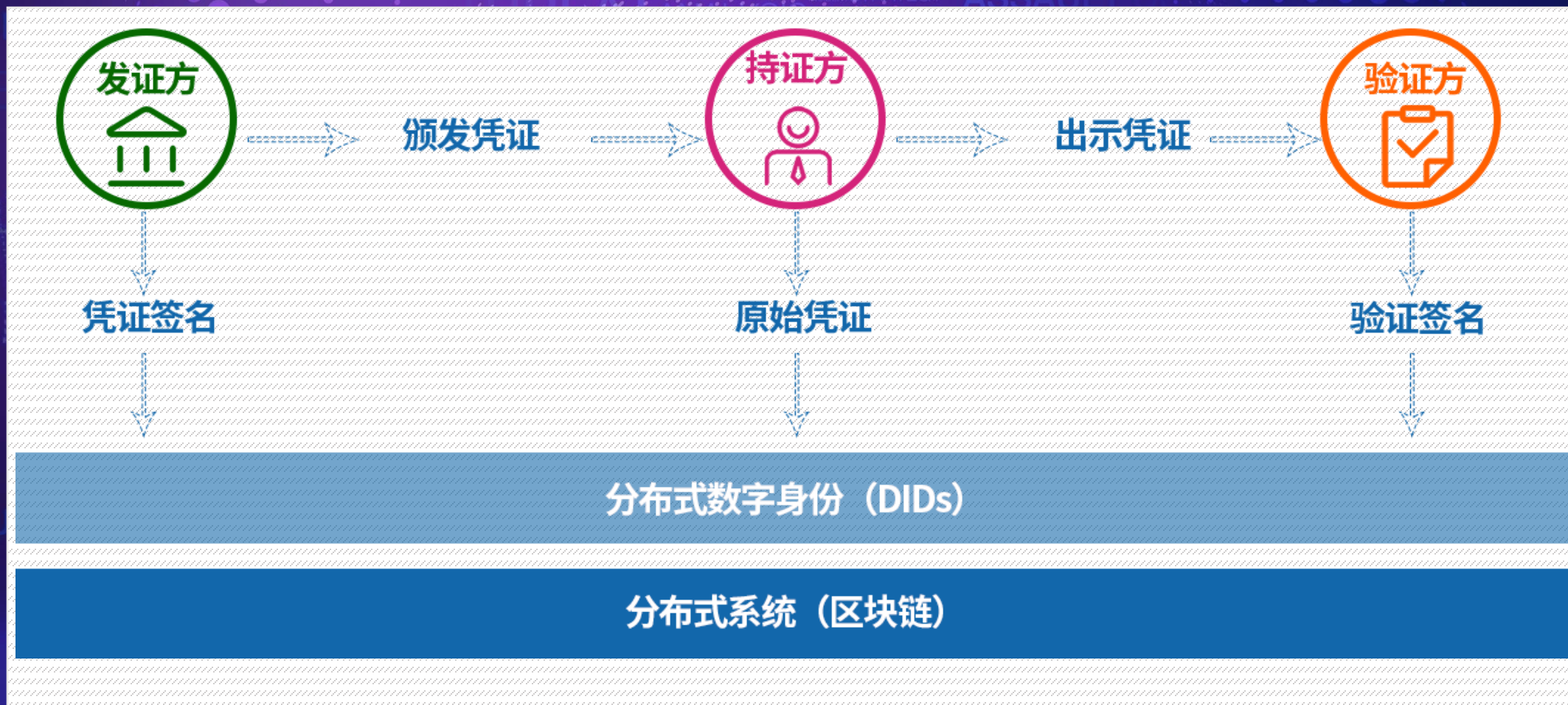


身份自主控制
任何存在于互联网上的实体都可以拥有一个完全属于自身的独立身份标识，互联网参与者可以更加便捷地使用和管理。

安全性高

分布式数字身份中，不含有用户真实的身份数据。避免敏感数据在互联网上进行传输时被不法分子盗用、窃取。







发证方

- 提供身份凭证的签发，具有一定数据公信力

其他

- 零知识证明算法、共识算法改造、云服务提供商等

区块链服务提供方

- 提供底层区块链技术支持

技术提供方

DID技术提供方

- 提供分布式数字身份技术支持

持证方

- 为用户提供凭证存储APP、硬件载体，以及与各方之间的对接

验证方

- 对凭证持有方进行验证，验证合法有效性



数字身份产业联盟(DIDA)创始单位



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



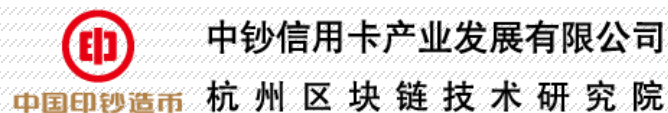
国家金融IC卡安全检测中心
National Financial IC Card Security Test Center
银行卡检测中心
Bank Card Test Center



杭州城市大脑有限公司
Hangzhou CityOS Co.,Ltd.



山东区块链研究院
SHANDONG INSTITUTE OF BLOCKCHAIN



中国银联电子支付研究院

(按字母排序, 排名不分先后)



深入研究分布式数字身份技术，包括去中心化公钥基础设施(DPKI)、区块链密码技术应用等



促进分布式数字身份的行业应用，搭建合作交流平台，组织产、学、研开展合作，探索分布式数字身份的应用场景



搭建中国的分布式数字身份网络，参考国际最佳实践，结合联盟成员的基础设施，以开源项目、制定团体标准等方式推进实施



与国际分布式数字身份接轨，成为本土企业与国际数字身份联盟和标准化组织的桥梁



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

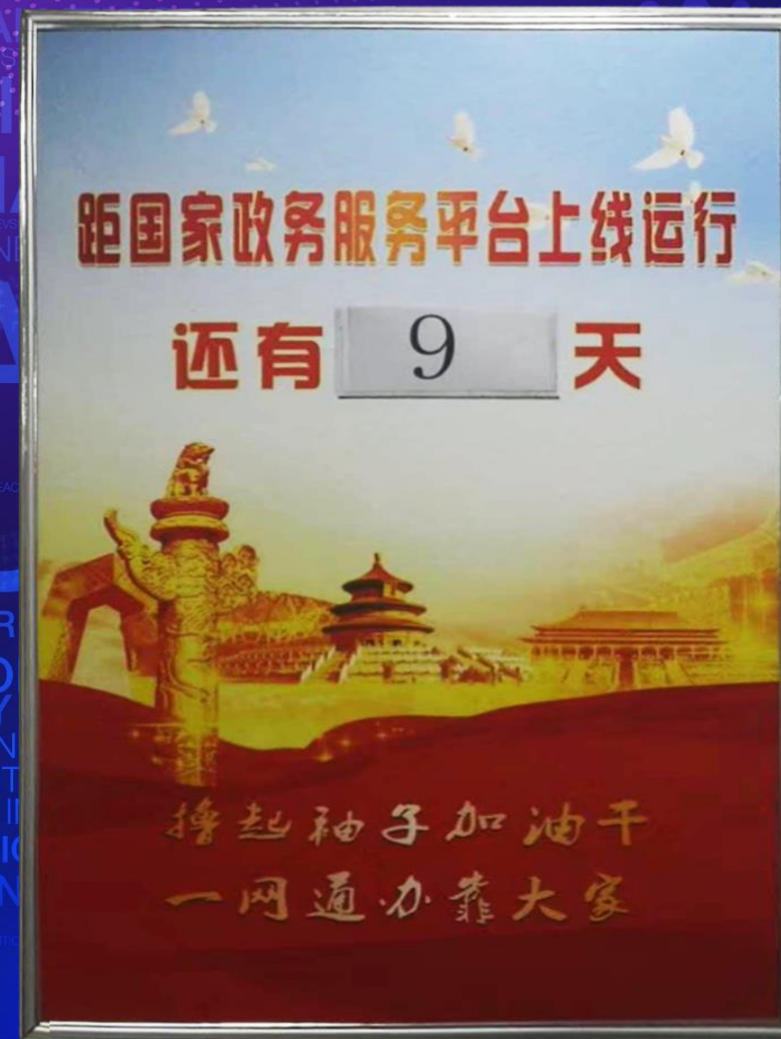


飞天诚信的实例：国家政务服务平台内网身份认证




“应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应采用密码技术实现”


——等保2.0三级以上要求（GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》8.1.4）






部署于包括近百套各类网络设备以及几千台主机、划分为四个区域、运行几十套应用系统的网络，为网络中的所有节点及应用系统提供使用密码技术的双因素身份认证服务，满足等保**2.0**三级要求

成熟可靠：拥有计算机信息系统安全专用产品销售许可证和商用密码产品认证证书，并通过权威第三方安全检测机构的检测，在超过**100**家金融机构使用

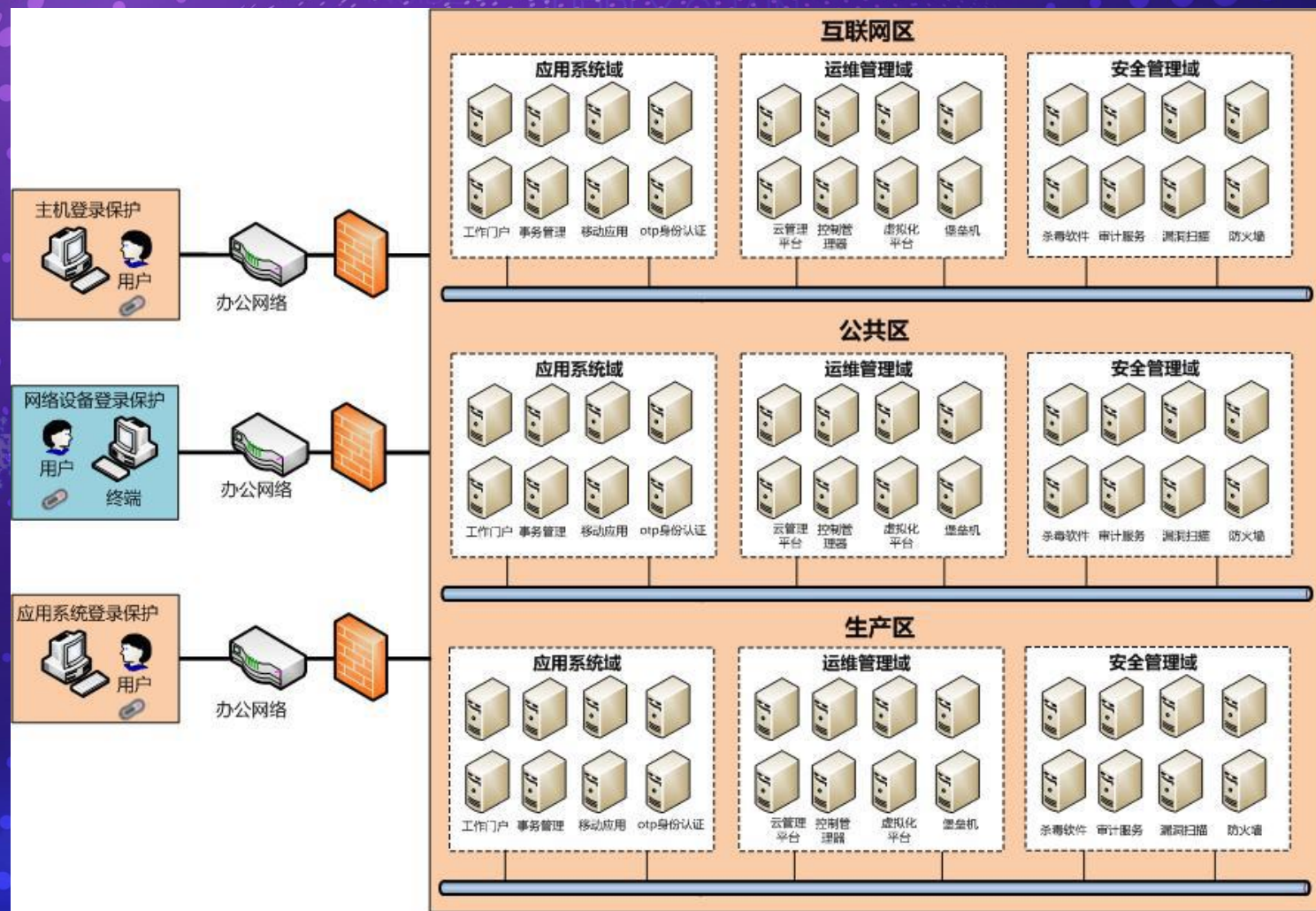
高性能：符合**GM/T 0021-2012**《动态口令密码应用技术规范》，认证速率超过**3000**次/秒（单节点）

部署方便：支持**Radius**协议，提供适配多种系统的认证代理软件用于对接；认证服务器支持独立部署和云上部署两种方式

飞天诚信的解决方案：自主可控的动态令牌认证系统



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



PERCONNECTED
ILITIES

HUMAN PROGRESS

DATA

BEHAVIORAL ANAL

TECHNOLOGY



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE



飞天诚信的呼吁： 产学研用携手，突破大规模分布式网络中密码应用的瓶颈



2020 北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANK YOU

全球网络安全 倾听北京声音