数字认证·共建可信任的数字世界

数字认证V2X安全证书服务解决方案

北京数字认证股份有限公司

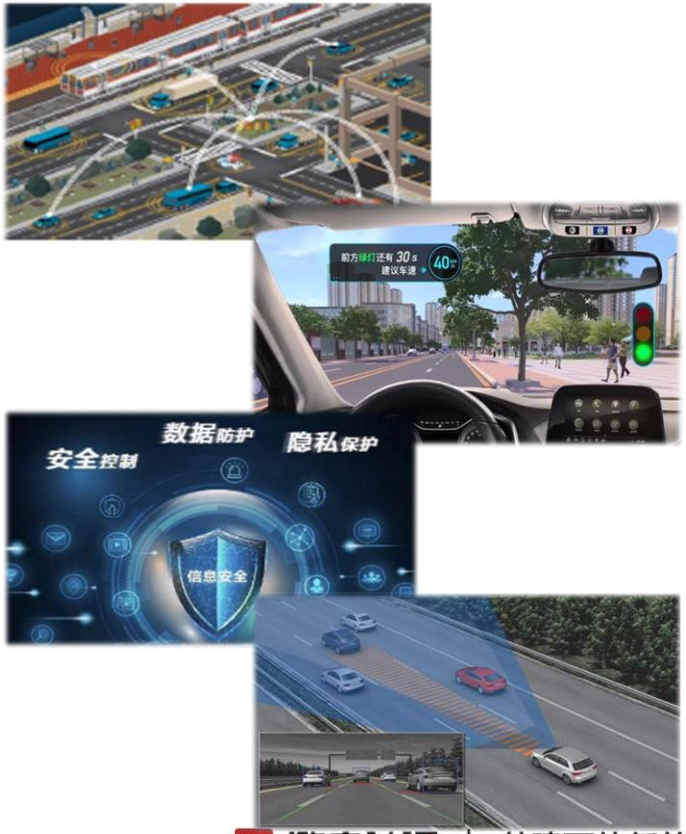
2021年1月

目 录
CONTENTS

车联网V2X安全背景

- C-V2X是车联网商业化部署应用的重要保障。车联网“人-车-路-云”通信过程中通过程中需要对车载设备、路侧基础设施等参与主体身份合法性性进行身份认证，消息认证，避免黑客一旦攻破或伪造消息，误导车辆作出错误判断，导致车辆碰撞等公共安全事件，造成比较恶劣的社会影响。

- 欧美等国家已研究并部署基于公钥基础设施（PKI）的V2X通信安全认证管理平台。国内相关研究尚处于起步阶段，在跨行业协同上也存在挑战，为加速车联网商业化部署，保证通信安全，应明确身份认证管理机构和管理机制，建立协同统一的安全认证管理平台。



车联网V2X面临的安全威胁和问题

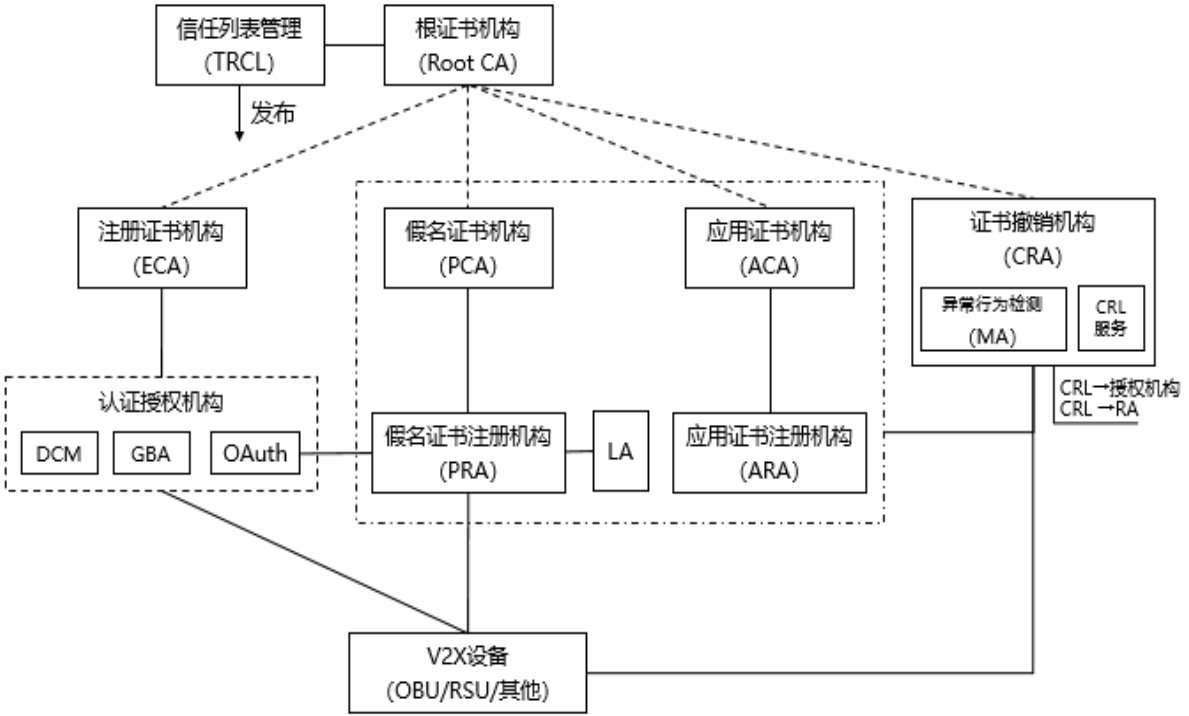
安全问题	安全威胁
通信内容伪造	误导接收者作出错误的决策或行动
通信内容删除	导致接收者不能根据当前路况作出正确的判断
通信内容重放	导致接收者根据不存的路面状况作出反应
通信凭证安全	身份泄露导致伪造V2X消息，影响车辆的决策
车辆隐私威胁	攻击者识别接收者的个人信息；长期位置跟踪。

安全防护策略

- 可信身份认证
- 消息完整性保护
- 消息抗重放保护
- 车辆标识匿名化

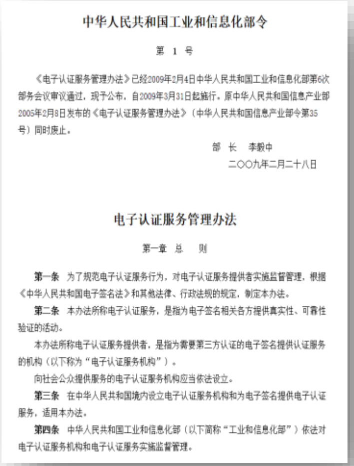
V2X安全证书应用

- 通过PKI/CA（数字证书）技术保障通信消息的可认证性、数据完整性、防篡改性、不可抵赖性；
- ECA为V2X设备提供注册证书申请、更新、吊销等服务；
- PCA为V2X设备（OBU）提供假名证书申请、证书下载服务；
- ACA为V2X设备提供应用证书和身份证书申请、下载服务；
- MA接收V2X上报的异常报告、报告检测分析及吊销列表签发。



提供具有法律效力的可靠电子认证服务

- 合规性要求：从事第三方电子认证服务的机构需要取得**电子认证服务使用密码许可证和电子认证服务许可证**，为能够为用户提供合法合规的电子签名服务；
- 电子认证服务机构应保证数字证书内容在有效期内真实、完整、准确，妥善保存与电子认证服务相关的信息，协助监管部门、司法、仲裁等机构的相关调查并提供必要信息等。



中华人民共和国工业和信息化部令

第 1 号

《电子认证服务管理办法》已经2009年2月4日中华人民共和国工业和信息化部第6次部务会议审议通过，现予公布，自2009年3月31日起施行。原中华人民共和国信息产业部2005年2月8日发布的《电子认证服务管理办法》（中华人民共和国信息产业部令第35号）同时废止。

部 长 李毅中

二〇〇九年二月二十八日

电子认证服务管理办法

第一章 总 则

第一条 为了规范电子认证服务行为，对电子认证服务提供者实施监督管理，根据《中华人民共和国电子签名法》和其他法律、行政法规的规定，制定本办法。

第二条 本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。

本办法所称电子认证服务提供者，是指为需要第三方认证的电子签名提供认证服务的机构（以下称为“电子认证服务机构”）。

向社会公众提供服务的电子认证服务机构应当依法设立。

第三条 在中华人民共和国境内设立电子认证服务机构和为电子签名提供电子认证服务，适用本办法。

第四条 中华人民共和国工业和信息化部（以下简称“工业和信息化部”）依法对电子认证服务机构和电子认证服务实施监督管理。

电子认证服务行业遵循运营管理规范要求

- **GB/T电子认证服务机构运营管理规范**
  - 运营系统、运营场地、安全组织、认证业务管理、记录审计、连续性控制
- **GB/T 35289-2017电子认证服务机构服务质量规范**
  - 服务质量要求（业务咨询、办理、技术支持、售后服务、司法支持）
  - 服务保障质量（场要求、组织机构人员、业务连续性）

目 录
CONTENTS

车联网V2X数字证书服务

数字认证作为第三方电子认证服务机构能够面向车端、路侧端以及车联网服务商提供数字证书服务，满足V2X车联网实体终端对数字证书的应用需求。

车联网V2X证书服务产品组成：

证书服务

- 注册证书、假名证书、身份证书和应用证书全生命周期管理服务
- CRL下载、证书链下载

支撑服务的相关产品

- 安全设备配置管理系统
- 终端安全中间件SDK
- 统一API网关平台
- 注册机构RA系统

01

证书服务

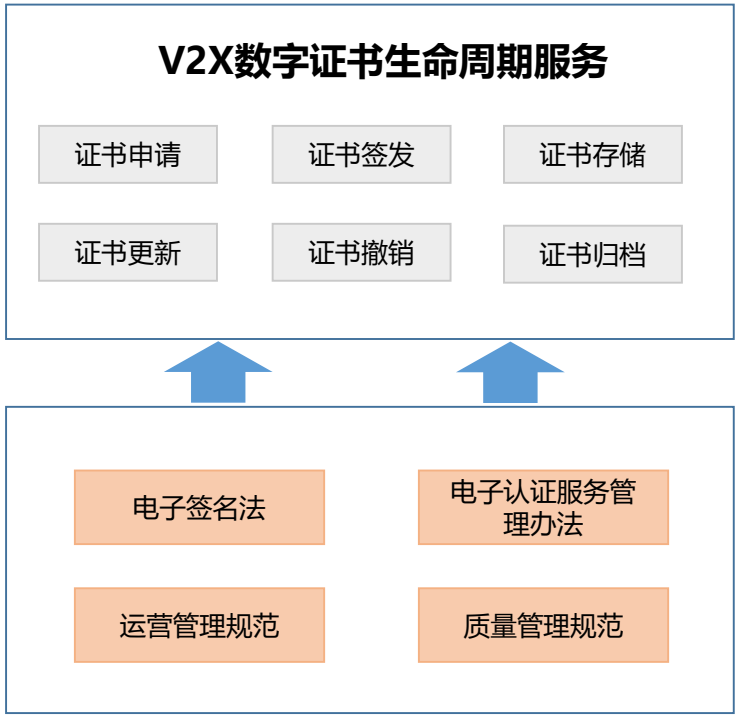
V2X数字证书服务类型

为V2X设备提供符合法律合规要求的各类证书服务。

证书类型包括注册证书、假名证书、身份证书和应用证书。

序号	证书类型	证书有效期	证书更新时间	使用对象及用途
1	注册证书	6年	任意时间	使用对象：车联网设备 用途：车联网设备的身份标识，用于请求假名、身份证书和应用证书
2	假名证书	一周	任意时间	使用对象：车载设备 用途：车载设备与车载设备通信交互时使用
3	身份证书	一月	任意时间	使用对象：车载设备 用途：车载设备与路侧设施通信交互时使用
4	应用证书	一月	任意时间	使用对象：路侧设施/VSP服务提供商 用途：路侧设施与路侧设施、车载设备通信交互时使用

V2X数字证书全生命周期服务



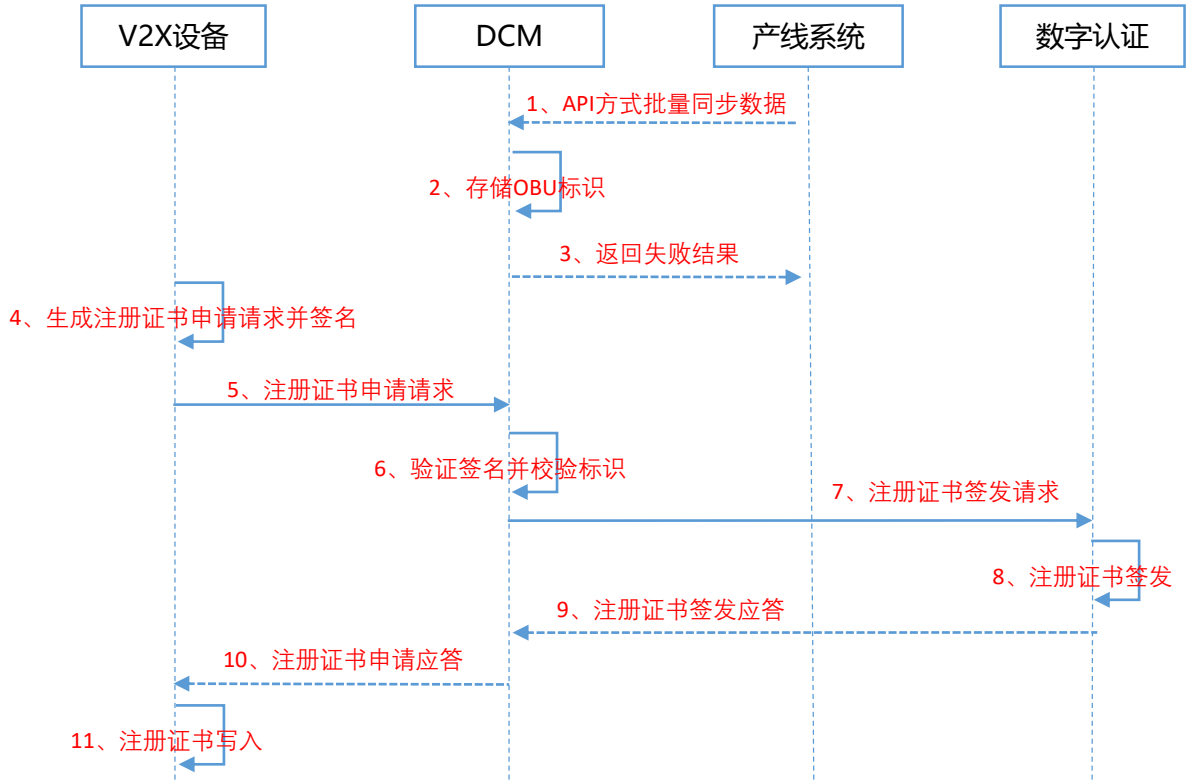
V2X申请注册证书服务

该服务是V2X设备基于DCM方式完成注册证书申请下载。

注册证书服务流程：

1、产线系统通过API方式将V2X设备的标识信息批量同步到DCM，DCM录入数据，并将录入结果返回产线系统；

2、OBU生成注册证书请求并签名，DCM申请校验，并完成后续注册证书申请下载应用。



V2X设备更新注册证书服务

该服务是在注册证书未到期的情况下为V2X设备设备申请新的注册证书。

注册证书更新服务流程：

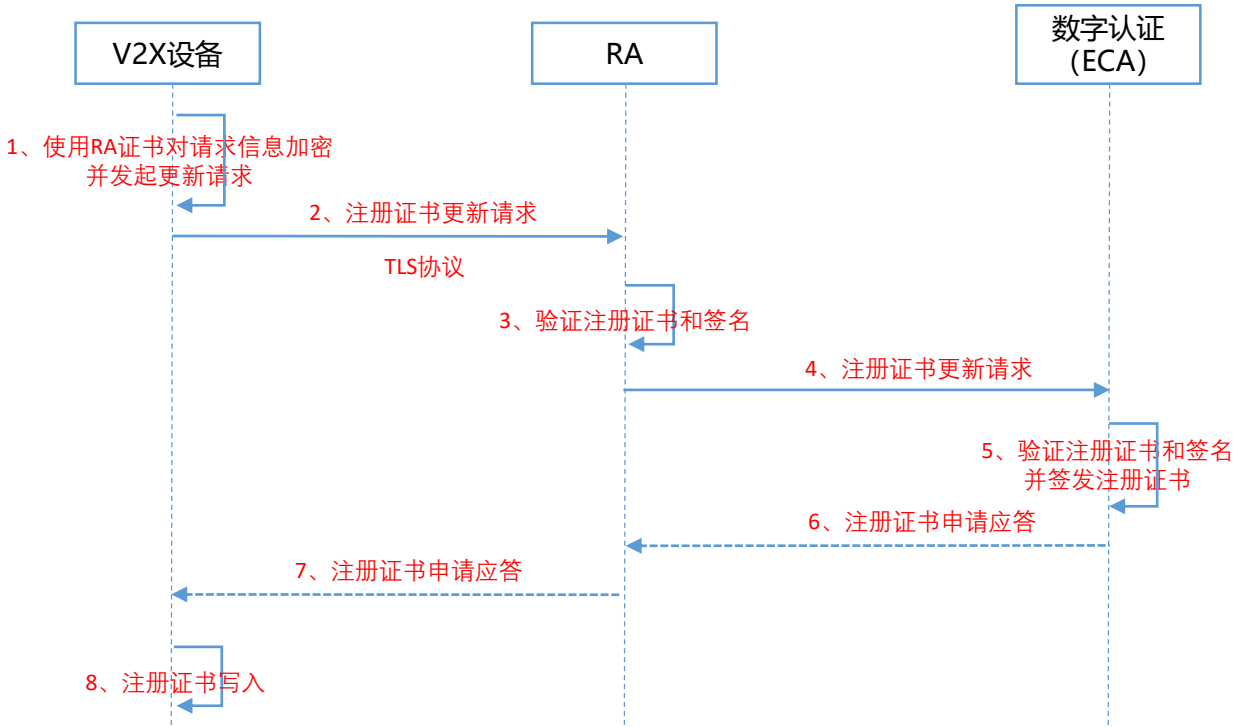
1、V2X设备向RA发起证书更新请求并加密；

2、RA接收解密并转发ECA；

3、ECA验证证书有效性和签名；

4、验证通过后，ECA签发EC证书，并发送证书响应消息；

5、V2X设备作废旧证书，并使用新的注册证书。



V2X申请假名证书服务

该服务是V2X设备基于EC证书签名申请假名证书的情况。

假名证书服务流程：

1、V2X设备生成假名证书PC申请请求，并使用注册证书EC对应的私钥对该请求进行签名；

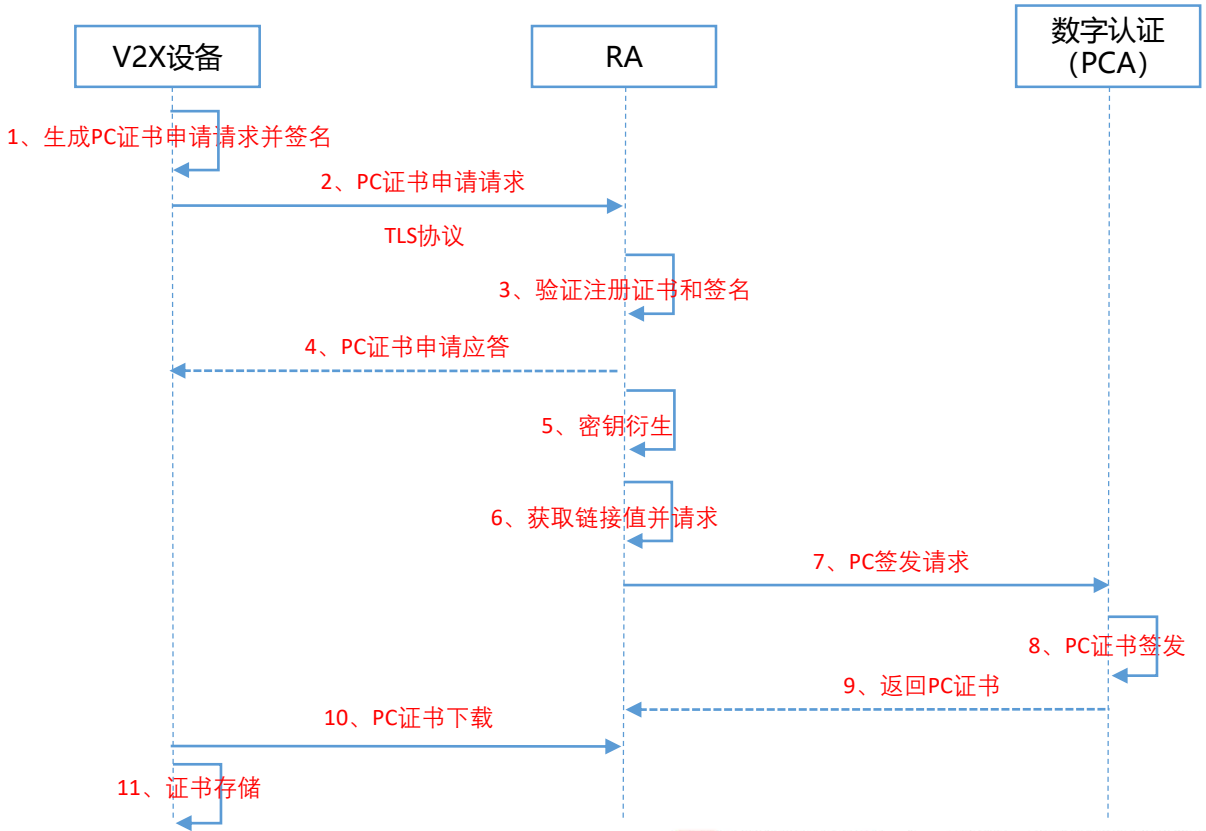
2、向RA发起假名证书申请请求，RA验证EC证书和签名；

3、验证通过后返回下载时间；

4、同时，RA对申请密钥做密钥扩展并获得链接值；

5、RA向PCA发起证书签发请求，PCA签发PC证书，返回RA，压缩存储；

6、V2X在下载时间内下载证书并存储。



V2X设备申请身份证书的业务场景

该服务是V2X设备基于EC证书签名申请身份证书，身份证书是OBU与RSU通信时对消息签名。

身份证书服务流程：

1、V2X设备生成身份证书申请请求，并使用注册证书EC对应的私钥对该请求进行签名；

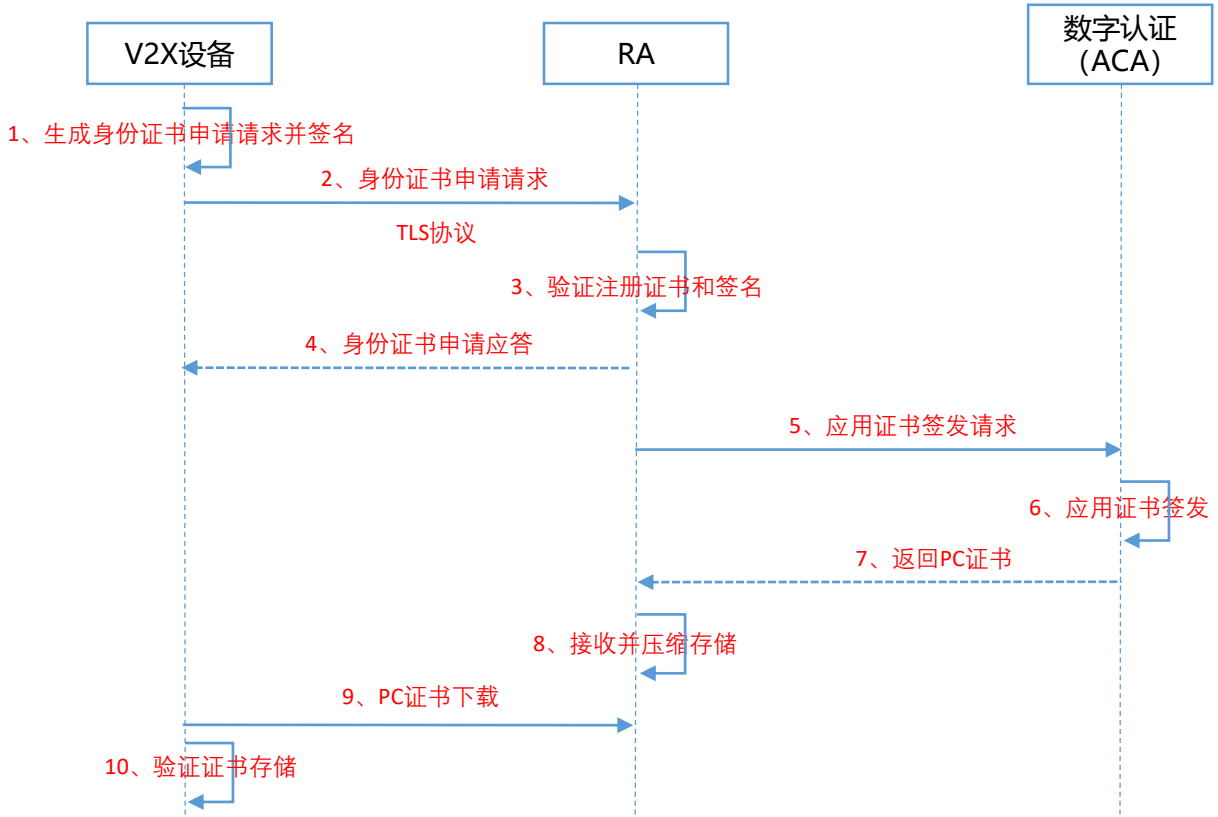
2、向RA发起身份证书申请请求，RA验证EC证书和签名；

3、验证通过后返回下载时间；

4、同时，RA向ACA转发身份证书签发请求；

5、ACA签发身份证书，返回RA，RA接收压缩存储；

6、V2X在下载时间内下载证书并存储。



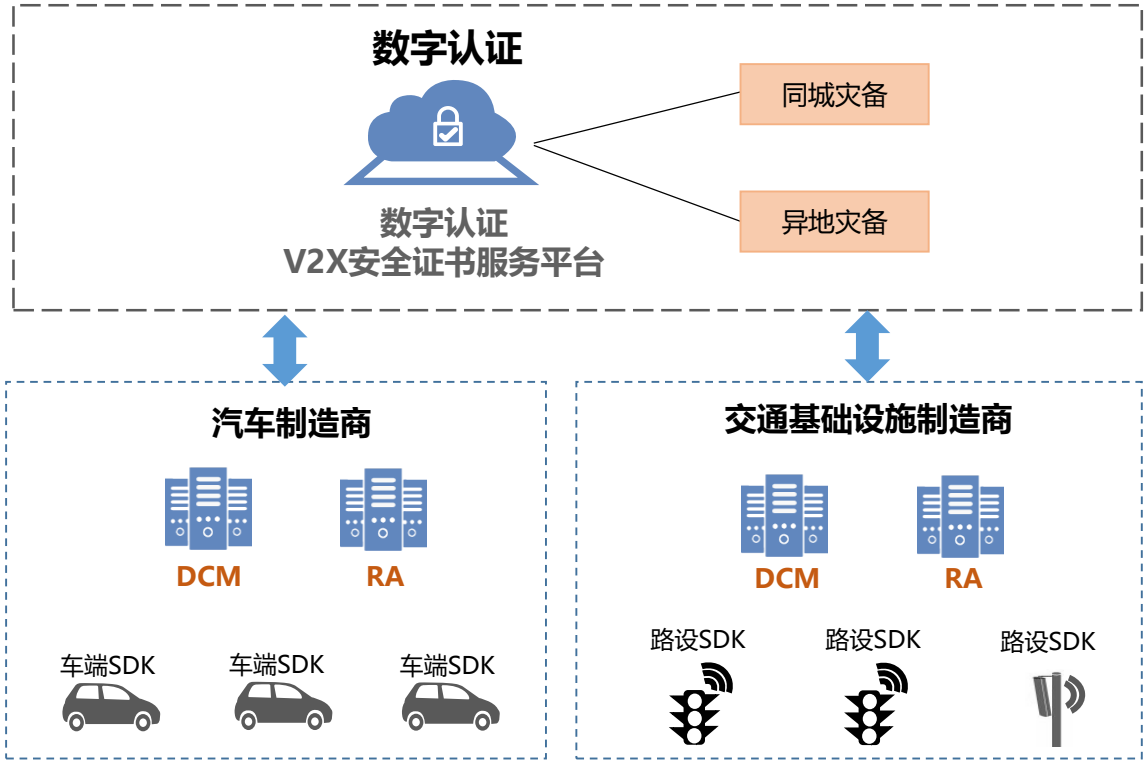
02

支撑服务相关产品

混合云部署服务方式

1、V2X证书管理系统核心服务采用屏蔽机房部署，接入层的网元可部署在汽车制造商或交通基础设施制造商云平台，面向V2X设备直接提供证书服务；

2、云平台和机房之间采用专线或VPN等安全接入方式，保障两者之间的链路安全。

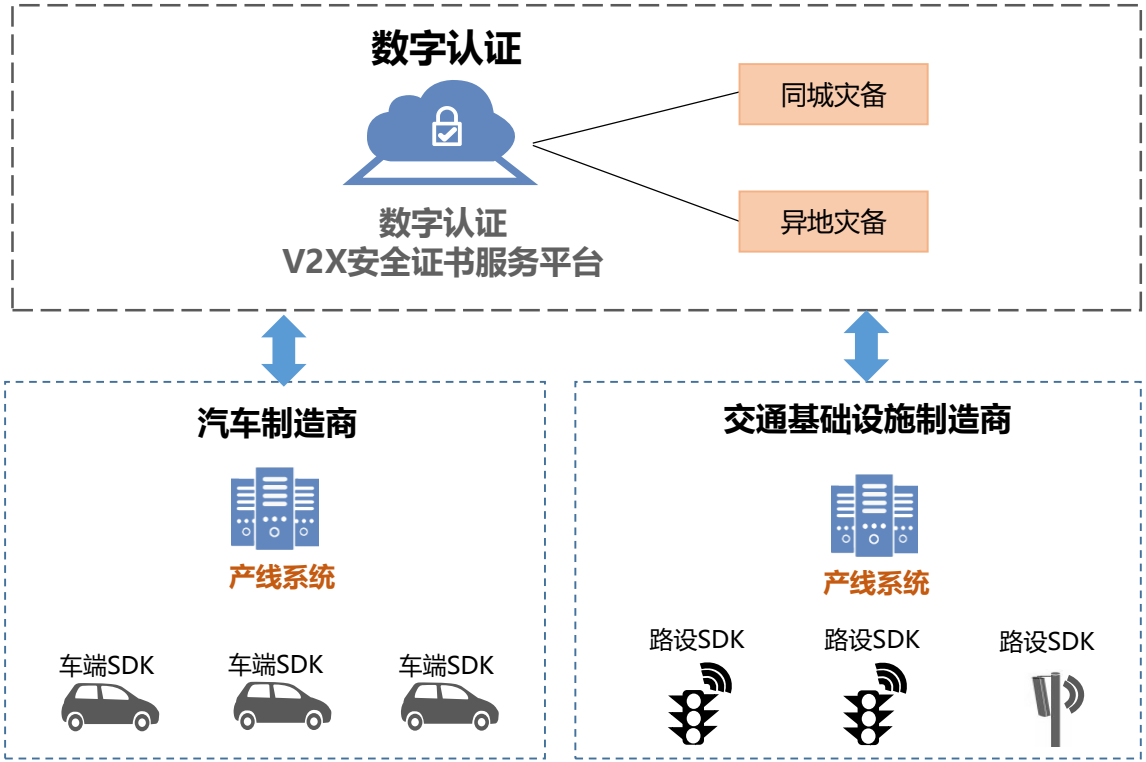


本地服务方式

1、依法成立的第三方电子认证服务机构。其发放的数字证书以及使用数字证书进行可靠的电子签名，均具法律效力。

2、采用“两地三中心”灾难恢复系统布局，即“一主两备”布局模式，保障系统安全可靠运行；

3、提供完善的运营服务支撑体系，保障服务高可用。

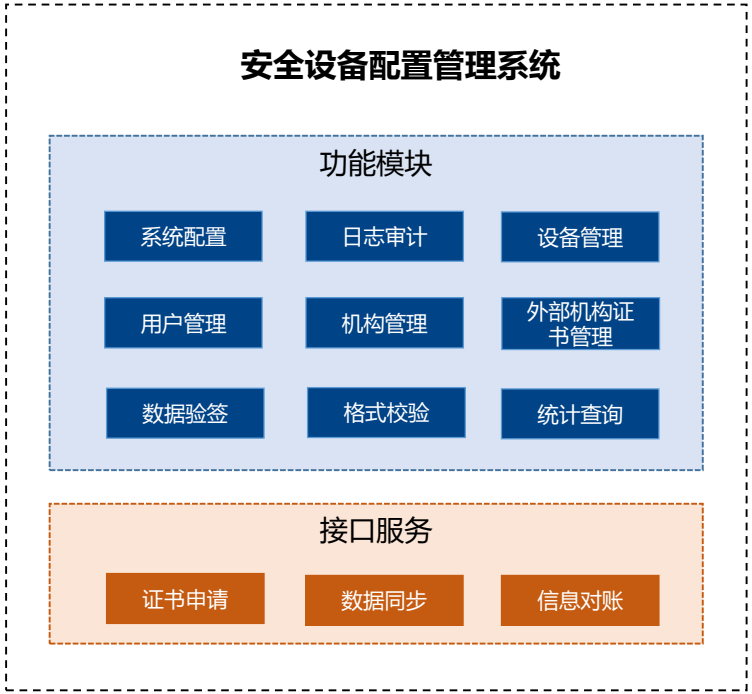


车联网V2X安全设备配置管理系统（DCM）

V2X设备通过DCM配置管理系统与注册证书机构交互，获取注册证书，基于 TLS安全协议建立安全的通信通道，确保V2X设备与DCM服务系统之间连接的安全性。整车厂、

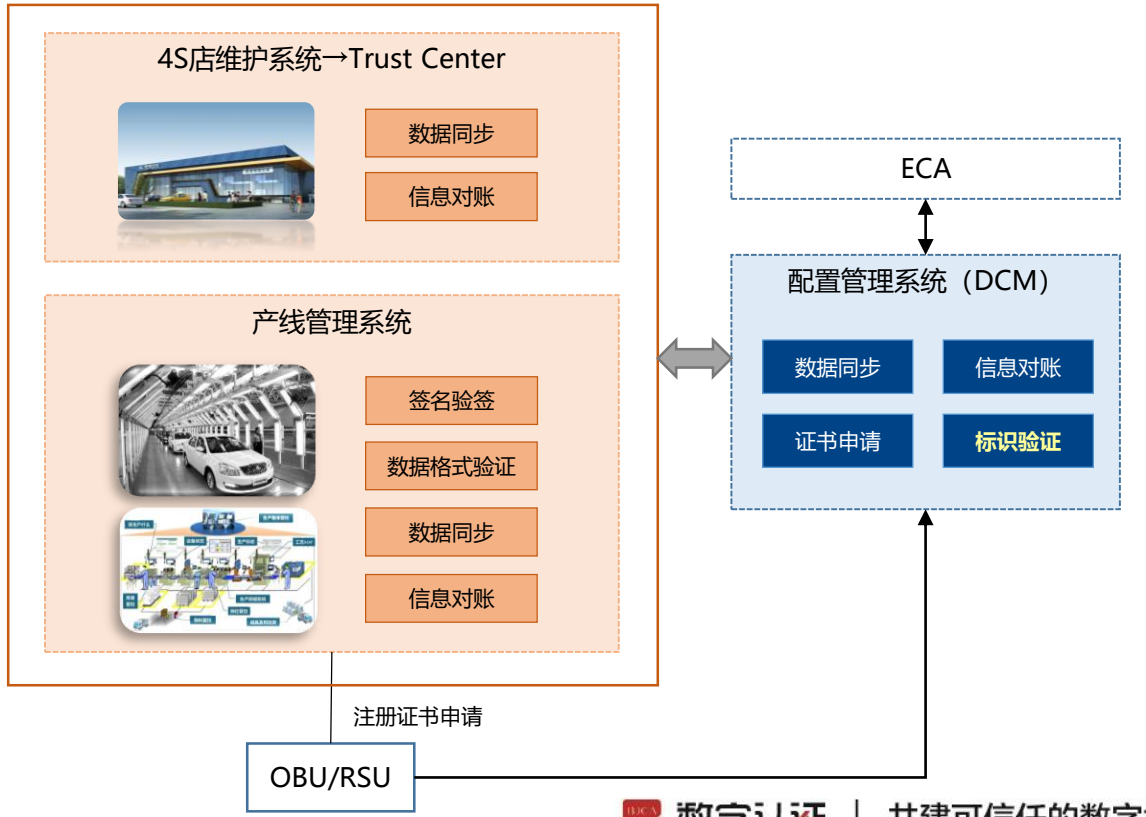
基础功能：

- 系统配置；
- 审计日志管理；
- 用户管理；
- 设备管理：终端设备信息维护、序列号校验配置；
- 机构证书管理；
- 外部机构证书管理，根CA导入；



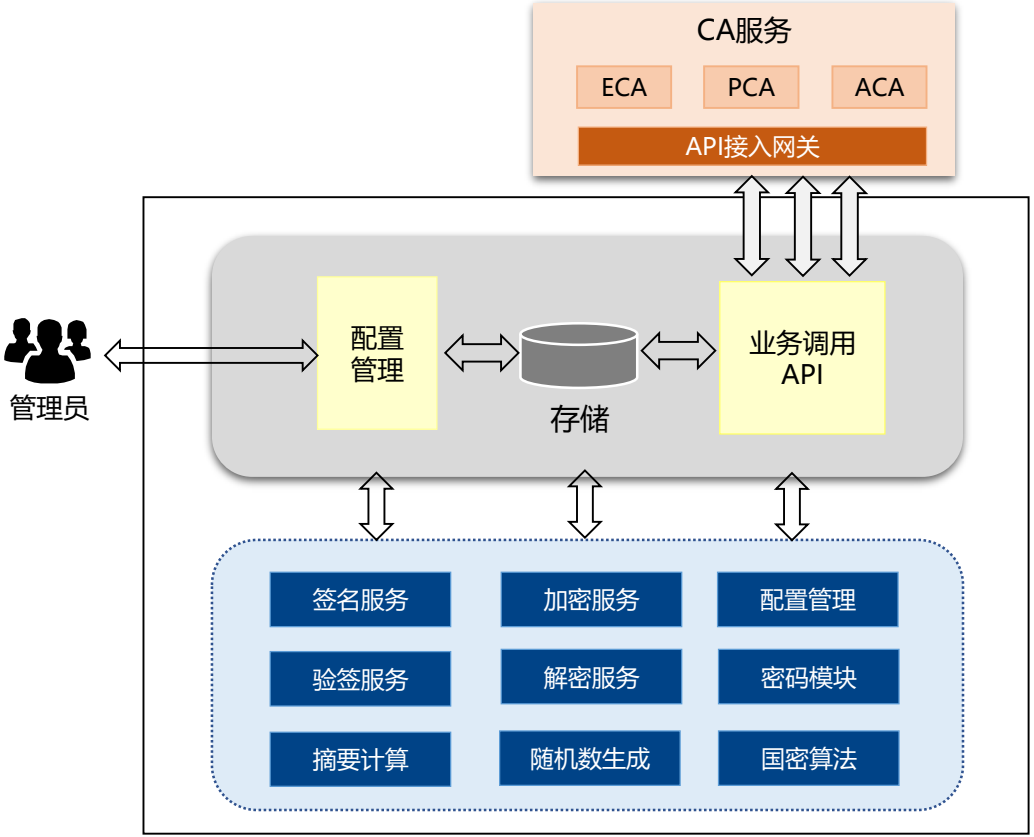
DCM与产线系统集成方案

- **注册证书申请方式**
  - OBU/RSU申请
  - 产线系统代理申请
- **系统改造**
  - 增加证书申请API
  - 数据同步API
  - 信息对账API
  - 功能性，签名验证和数据格式验证



车联网V2X终端安全中间件软件

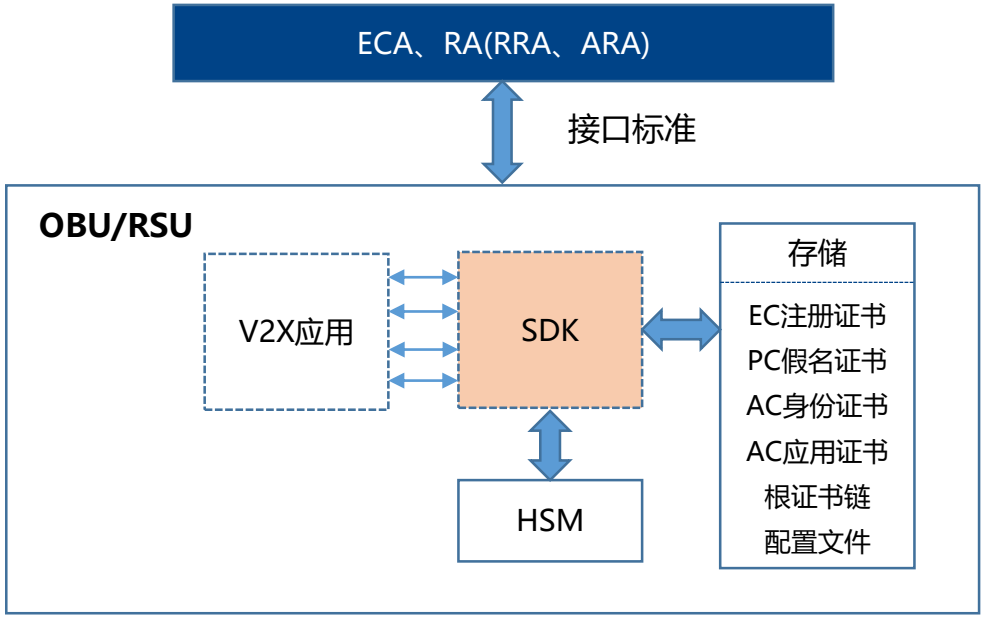
- 针对车联网V2X设备，提供证书相关及密码服务相关的V2X终端安全软件SDK集成包，通过终端SDK与平台层进行数据交互，完成证书服务相关业务。
- 提供与OBU及RSU等嵌入式系统集成和二次开发，以及密钥、证书的生命周期管理及应用开发接口。



V2X设备与终端安全中间件软件集成方案

对接API：

- 注册证书申请
- 注册证书更新
- 假名证书申请
- 假名证书下载
- 应用证书申请
- 应用证书下载
- 身份证书申请
- 身份证书下载
- 证书链下载
- CRL下载
- 签名验签
- 加密解密



统一API网关平台

- **API生命周期托管**

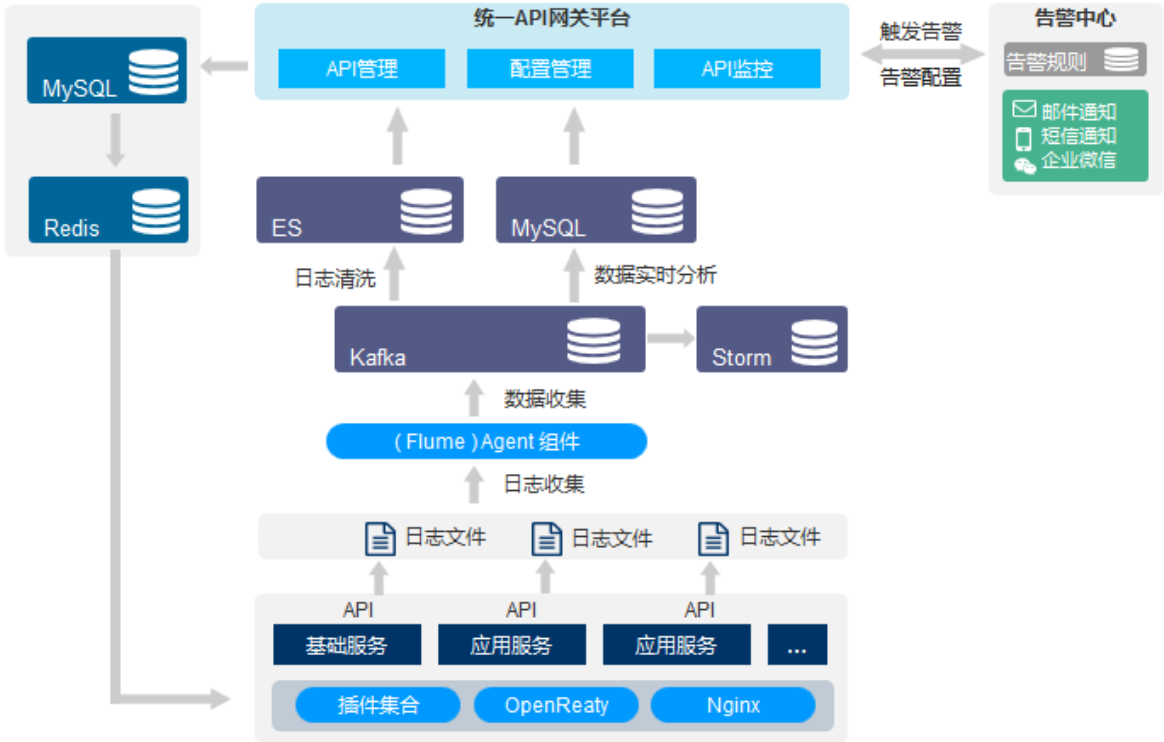
统一API网关平台对外网的安全隔离，可以完成API的整个生命周期的托管，包括创建、版本管理、发布、上线、下线、监测、销毁等。

- **授权管理**

接口授权认证，参数流量控制，统一的日志管理。

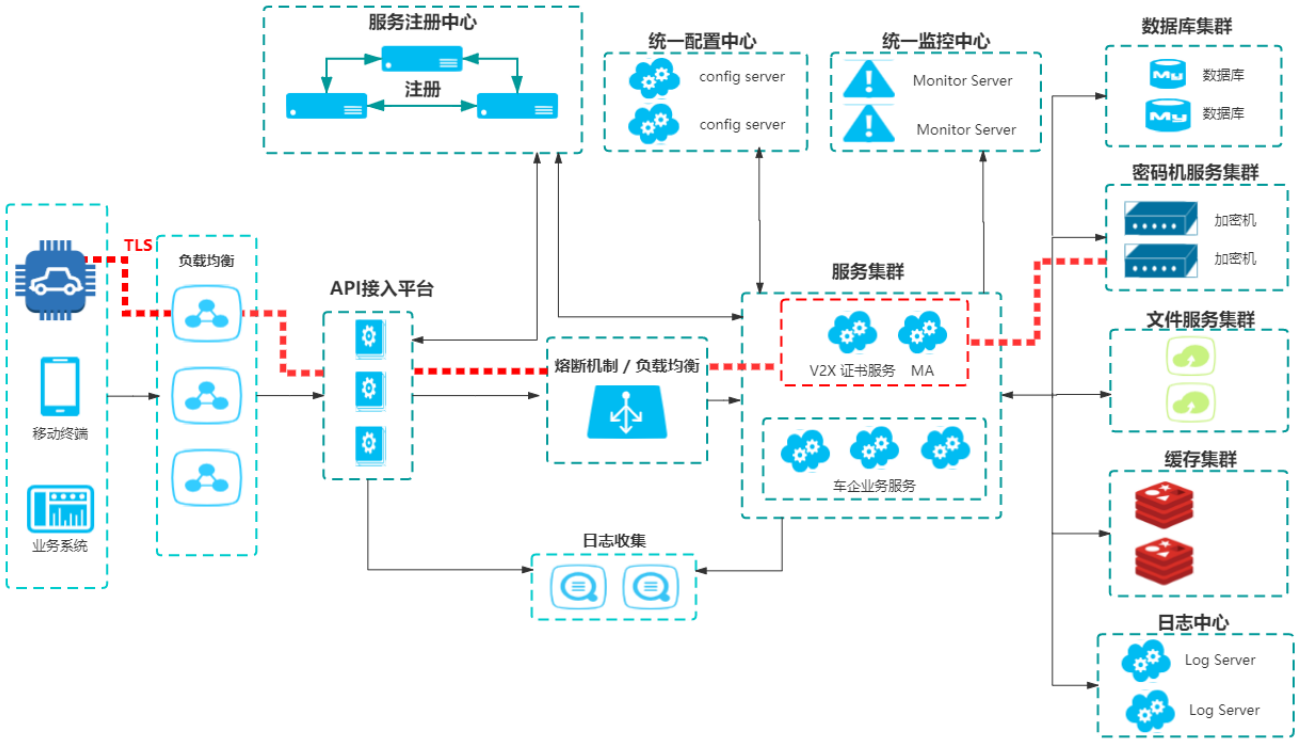
- **监控统计**

调用统计，用量、响应时间、错误率、网络情况等。集合统计监控预警，配置报警策略。



平台架构具备安全服务高可用及水平扩展能力

- 安全隔离；
- 服务高可用；
- 支持水平扩展；
- 统一接入，统一监管；
- 增值服务



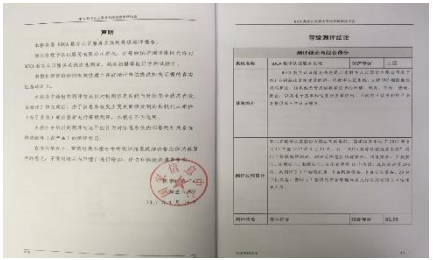
目 录
CONTENTS

CA运营服务全方位的资质证书

电子认证服务许可证

电子政务电子认证服务机构

电子认证服务使用密码许可证



公安部等保三级测评报告

ISO27000信息安全管理体系认证

ISO27018个人信息安全管理体系认证

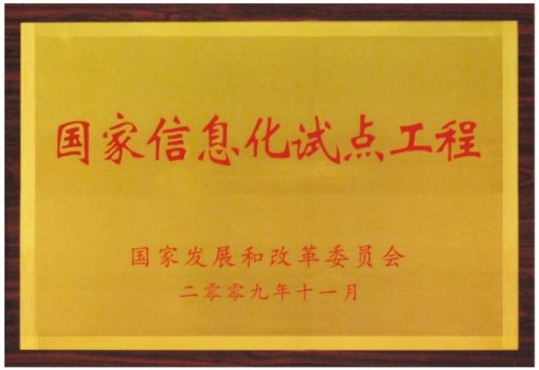
信息安全风险评估服务资质

信息安全应急处理服务资质

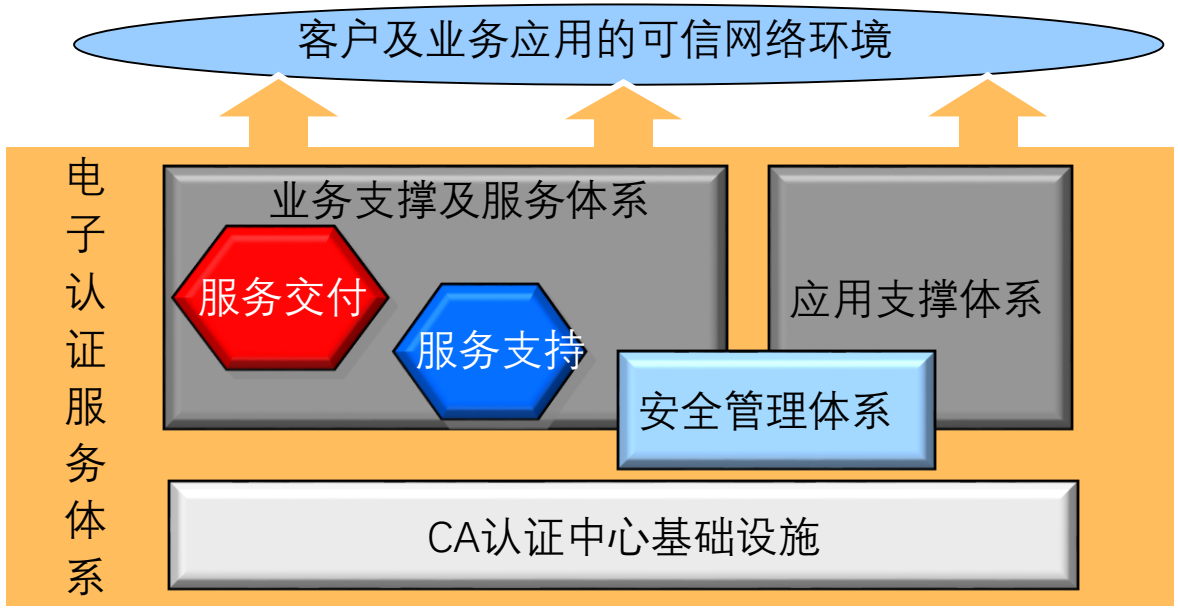
核心理念：以“客户为中心“的新型电子认证服务体系

服务宗旨：可信规范的运营，随需应变的服务

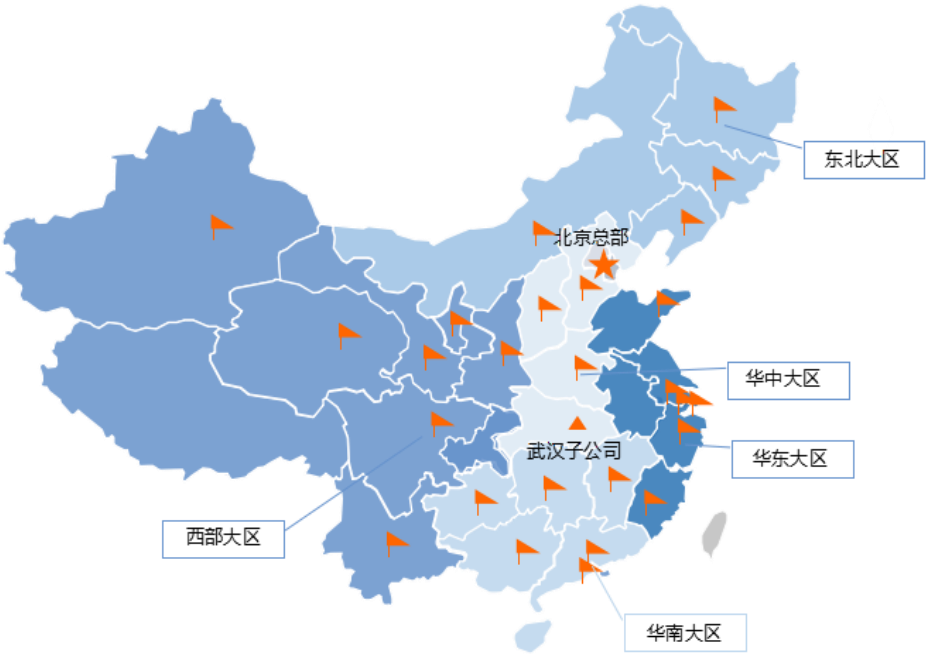
服务能力：自主知识产权的技术体系，面向客户的综合服务体系



2009年，BJCA“以客户为中心的新型电子认证服务体系”在国家发改委信息化试点示范工程中排名电子认证服务试点第一名，获得国家资金重点支持
2012年，获国家密码局科学进步二等奖



电子认证服务-运营服务规模与能力



公司证书服务网点覆盖全国32个省市，建立了京津、华东、华南、华中、东北、西部6个大区和分公司，全国共有20多个办事处，60多家合作伙伴。

全国范围有上千个自营和渠道服务网点，证书服务渠道超过1400个。

拥有近200人组成的专业、经验丰富的运营服务团队，具有多个国家部委、大型机构的服务经验。

电子认证服务-运营服务规模与能力

各类证书年度发证量超过5亿张。

云签名服务年度签名量超过1.16亿次。

系统能够支撑十亿级的服务能力。

支持7*24小时99.99%的系统可用性。

系统运维管理-安全运维管理体系

ISO 27000信息安全体系认证

人员安全

- CA机构可信人员背景调查、公安机构无犯罪记录证明。

系统安全

- 定期渗透测试、漏洞扫描和防病毒检测，以及安全加固。

网络安全

- 部署抗DDOS攻击、入侵防御、防火墙和VPN等安全设备。

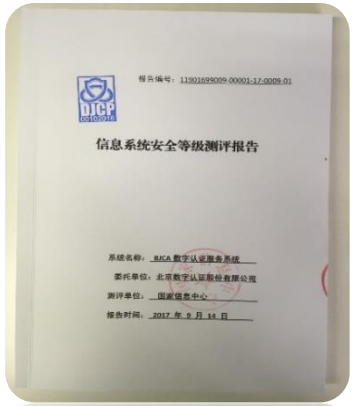
密钥安全

- 符合国家密码主管部门安全要求与规定。

物理安全

- 建设屏蔽机房，以及环控、安保、配电合消防等全方位安全监控系统。

信息系统安全等级保护三级

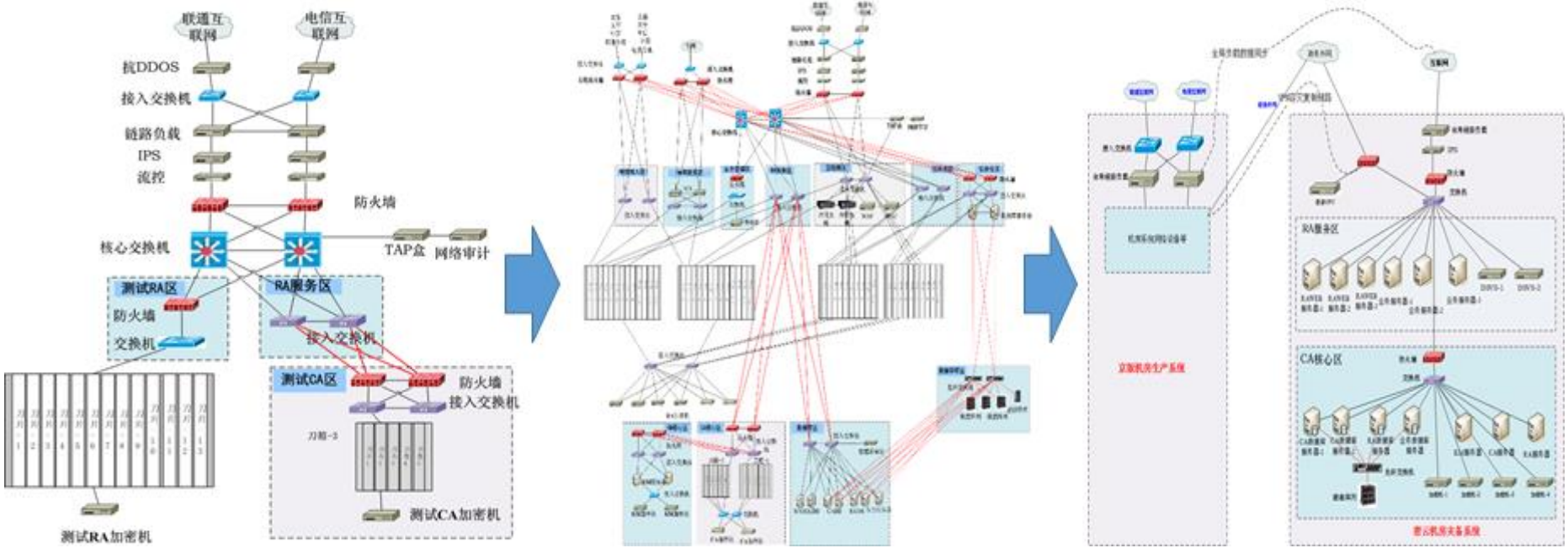


运营服务管理制度

1	**北京市法人一证通证书制度规范**		
1.1	北京法人一证通管理暂行办法	QP	Q-ZSFW-OS-QP-1-2016
1.2	北京市法人数字证书使用管理办法（试行）	QP	Q-ZSFW-OS-QP-2-2016
1.3	北京市法人一证通电子认证业务规则	WI	Q-ZSFW-OS-WI-1.1-2016
1.4	北京市法人一证通项目服务质量管理规范	WI	Q-ZSFW-OS-WI-1.2-2014
1.5	北京市法人一证通用户资料管理规范	WI	Q-ZSFW-OS-WI-1.3-2016
2	**中国移动证书服务制度规范**		
2.1	BJCA合作伙伴电子认证服务管理办法（专用）	QP	Q-ZSFW-OS-QP-3-2015
2.2	中国移动电子采购与招标投标系统CA证书使用管理办法	QP	Q-ZSFW-OS-QP-4-2015
2.3	招投标类证书工作规范（合作伙伴版）	WI	Q-ZSFW-OS-WI-2.1-2016
2.4	招投标类证书工作规范（BJCA自营版）	WI	Q-ZSFW-OS-WI-2.2-2016
3	**自营模式证书服务制度规范**		
3.1	BJCA证书鉴证白皮书	WI	Q-ZSFW-OS-WI-3.1-2010
3.2	受理点现金管理制度	QP	Q-ZSFW-OS-QP-5-2017
3.3	受理点备用金管理制度	QP	Q-ZSFW-OS-QP-6-2017
3.4	BJCA证书类存货及发票丢失处理办法	WI	Q-ZSFW-OS-WI-3.2-2014
3.5	公务用车管理制度	QP	Q-ZSFW-OS-QP-7-2017
4	**合作伙伴模式证书管理制度规范**		
4.1	BJCA合作伙伴电子认证服务管理办法	QP	Q-ZSFW-OS-QP-8-2015
4.2	合作伙伴运营管理制度	QP	Q-ZSFW-OS-QP-9-2014
4.3	合作伙伴受理点管理制度	QP	Q-ZSFW-OS-QP-10-2014
5	**服务质量监督制度规范**		
5.1	服务审计规范	QP	Q-ZSFW-OS-QP-11-2014
5.2	BJCA内部服务质量监督管理制度	QP	Q-ZSFW-OS-QP-12-2015
5.3	合作伙伴务质量监督管理制度	QP	Q-ZSFW-OS-QP-13-2015
6	**物料库房管理制度规范**		
6.1	库房管理制度	QP	Q-ZSFW-OS-QP-14-2014
6.2	介质质量问题反馈管理制度	QP	Q-ZSFW-OS-QP-15-2016

1	**BJCA运维安全管理体系**	QP	CA-SO-QP-1
1.1	BJCA数字认证服务系统信息安全方针和策略	WI	CA-SO-WI-1.1
1.2	BJCA数字认证服务系统信息安全管理制度制定与发布	WI	CA-SO-WI-1.2
1.3	BJCA数字认证服务系统信息安全组织机构及职责	WI	CA-SO-WI-1.3
1.4	BJCA数字认证服务系统数据查询与修改审批管理制度	WI	CA-SO-WI-1.4
1.5	BJCA数字认证服务系统信息安全检查与监督制度	WI	CA-SO-WI-1.5
1.6	BJCA数字认证服务系统人员安全管理制度	WI	CA-SO-WI-1.6
1.7	BJCA数字认证服务系统安全教育培训管理制度	WI	CA-SO-WI-1.7
1.8	BJCA数字认证服务系统建设管理制度	WI	CA-SO-WI-1.8
1.9	BJCA数字认证服务系统机房环境管理制度	WI	CA-SO-WI-1.9
1.10	BJCA数字认证服务系统日常值班管理制度	WI	CA-SO-WI-1.10
1.11	BJCA数字认证服务系统资产管理制度	WI	CA-SO-WI-1.11
1.12	BJCA数字认证服务系统介质管理制度	WI	CA-SO-WI-1.12
1.13	BJCA数字认证服务系统设备管理制度	WI	CA-SO-WI-1.13
1.14	BJCA数字认证服务系统安全监控管理制度	WI	CA-SO-WI-1.14
1.15	BJCA数字认证服务系统网络安全管理制度	WI	CA-SO-WI-1.15
1.16	BJCA数字认证服务系统安全管理制度	WI	CA-SO-WI-1.16
1.17	BJCA数字认证服务系统防病毒管理制度	WI	CA-SO-WI-1.17
1.18	BJCA数字认证服务系统密码管理制度	WI	CA-SO-WI-1.18
1.19	BJCA数字认证服务系统备份与恢复管理制度	WI	CA-SO-WI-1.19
1.20	BJCA数字认证服务系统变更管理制度	WI	CA-SO-WI-1.20
1.21	BJCA数字认证服务系统安全事件管理制度	WI	CA-SO-WI-1.21
1.22	BJCA数字认证服务系统应急预案管理制度	WI	CA-SO-WI-1.22

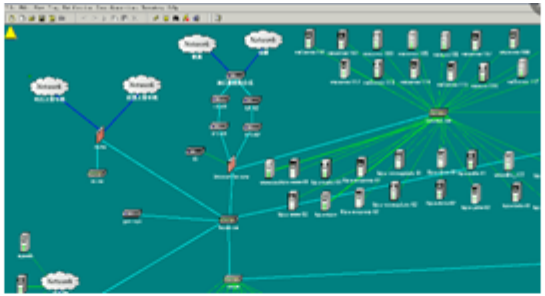
系统运维管理-完善测试、生产和备份环境



预上线系统　　生产系统　　容灾备份系统

系统运维管理-全方位运维监控

网络边界带宽监控



网络运行全局监控

服务器群监控

应用系统日志监控

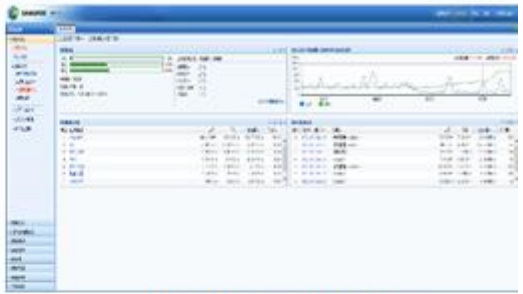
埋点与探针监控

应用系统性能监控

系统运维管理-外部安全防护

抗DDOS攻击系统

IPS网络防御监控



网络流量控制系统

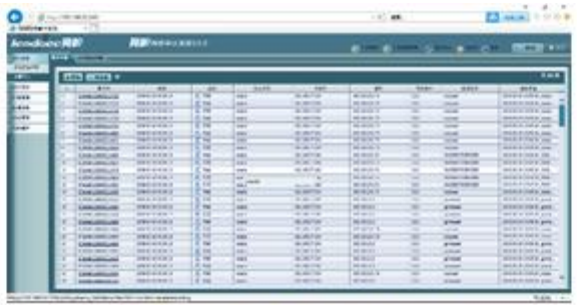
网络防火墙系统

WAF网站防御系统

网页防篡改系统

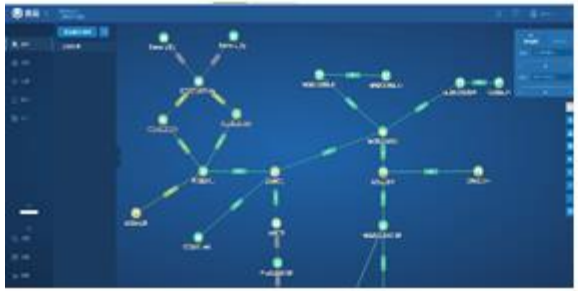
系统运维管理-内部安全防护

网络内部审计系统



数据库内部审计系统

回溯查询系统

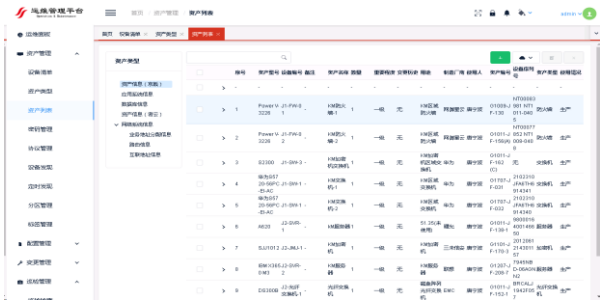


优云网络安全管理系统

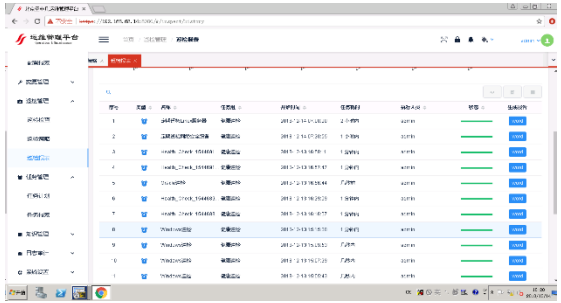
运维安全堡垒机

防病毒监控平台

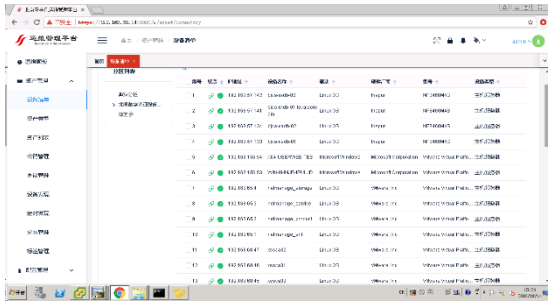
系统运维管理-自动化运维+监控告警



台账自动化管理



运维自动化巡检



自动化运维脚本

邮件告警

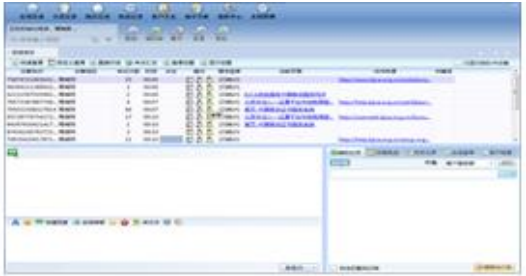
短信告警

微信告警

“以客户为中心”的客户服务模式

大客户直通车网站

热线客服



在线客服

微信客服

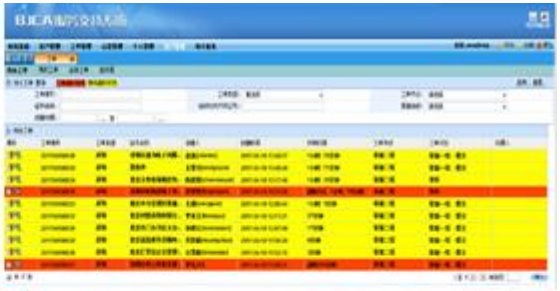
邮件客服

实时短信

客服服务信息化管理-规范、先进、流程化

热线实时接通率管理

在线客服实时监控



客服工单实时监控

客服热线知识库管理

客服热线录音质检管理

热线实时满意度管理

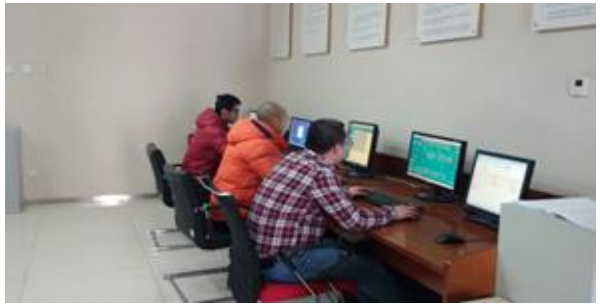
运维信息化管理-运维规范流程化、系统化

系统变更上线流程管理

7*24小时运维交接班记录与管理

运维管理审批流程

业务连续性保障-容灾备份恢复演练结果



2017年度容灾演练

2018年度容灾演练

2017年BJCA CA系统同城灾备演练操作步骤记录表（京版到密云）

日期：2017年11月4日

序号	操作内容	操作人员	操作时间	操作结果	签名
1	启用京版CA交换机ACL访问策略	王德臣	23:00	正常	王德臣
2	停止京版向密云的数据同步服务	覃光荣	23:01	正常	覃光荣
3	修改密云机房DNS域名映射关系优先级为高优先级	王德臣	23:02	正常	王德臣
4	启用密云机房对外服务防火墙允许访问策略	王德臣	23:04	正常	王德臣
5	密云灾备系统访问测试	李万龙	23:05	正常	李万龙
6	检查数据一致性	覃光荣	23:07	正常	覃光荣
7	执行最后10条发证信息执行检查证书签发状态	寇振方	23:09	正常	寇振方
8	业务测试	常松	23:06-2:00	正常	常松
9	京版到密云演练完成	孙国福	2:30	正常	孙国福

演练实际操作记录

北京数字认证股份有限公司
BEIJING CERTIFICATE AUTHORITY

北京银行OTP个人证书渠道切换测试结果

序号	测试点	测试内容	测试时间	测试结果	测试员签字
1	证书下载	新办	20171104	通过	

北京银行OTP个人证书渠道切换测试结果

序号	测试点	测试内容	测试时间	测试结果	测试员签字
1	证书下载	新办	20171105	通过	

北京银行企业网银渠道切换测试结果

序号	测试点	测试内容	测试时间	测试结果	测试员签字
1	证书制作（离线）	新办	20171104	通过	
2		密码卡回收	20171104		

北京银行企业网银渠道切换测试结果

序号	测试点	测试内容	测试时间	测试结果	测试员签字
1	证书制作（离线）	新办	20171105	通过	
2		密码卡回收	20171105		

北京银行银企直联渠道切换测试结果

序号	测试点	测试内容	测试时间	测试结果	测试员签字
1	证书制作（离线）	新办	20171104	通过	
2		丢失补办确认吊销列表	20171104		
3		密码卡回收	20171104		
4	证书制作（在线）	在线解锁	20171104		

北京银行银企直联渠道回切测试结果

序号	测试点	测试内容	测试时间	测试结果	测试员签字
1	证书制作（离线）	新办	20171105	通过	
2		丢失补办确认吊销列表	20171105		
3		密码卡回收	20171105		
4	证书制作（在线）	在线解锁	20171105		

演练实际测试结果

目 录
CONTENTS

数字认证V2X车联网服务体系在整车厂的完整实践案例

数字认证在V2X车联网数字证书应用方面拥有丰富的成功实践经验，在此基础上，融合大规模商用证书运营服务经验以及车联网安全认证技术体系，为客户提供基于PKI/CA技术的安全证书服务，满足车联网应用场景下的安全需求。

- **服务于国际知名车企的车联网数字证书安全认证系统平台建设项目**

本项目是数字认证与华为技术公司合作，构建安全证书服务平台，为国际知名车企提供”两地三中心” 电信运营级商用数字证书服务。

- **服务于东风汽车集团的车联网数字证书安全认证系统建设项目**

中标承建东风汽车集团科技公司襄阳达安车联网数字证书安全认证系统建设项目，构建X.509 PKI体系和V2X PKI体系，结合车云、车车、车路交互业务应用场景详细设计，实现各实体终端基于数字证书的身份鉴证、设备数字身份管理、通信数据安全、通信信道安全、密钥存储安全等安全需求，满足智能网联汽车安全应用。

- **服务于上汽集团的PKICA体系建设项目**

数字认证承建了上汽集团的科技公司斑马网络车联网PKI/CA体系建设项目为上汽集团品牌汽车TSP平台、T-BOX终端、APP 终端、云端用户、设备厂商企业等发放各类数字证书。

- **华晨宝马数字证书应用项目**

数字认证与华晨宝马汽车签署各类数字安全证书服务合同，为华晨宝马提供数字认证服务，为车载终端应用提供全方位技术支持服务。

- **深圳坪山智能网联交通产业示范区车联网安全证书服务项目**

为广汽集团下属品牌车辆和比亚迪车辆提供安全证书服务。解决先导示范区车联网典型应用场景下的身份认证、消息认证、隐私保护等问题。

谢 谢

THANKS

数字认证 | 共建可信任的数字世界