密码基础产品与密码测评中的应用

主讲人：张秋璞

目录

CONTENTS

赢达信 YDXSAFE

公司介绍

PART. 01

公司简介

天津赢达信科技有限公司，是一家以密码和移动互联网技术为核心，提供终端安全、云安全应用、数据安全服务、工控安全和金融安全的高科技公司。

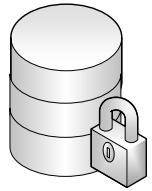
- ✓注册资金人民币2000万元
- ✓高新技术企业资质证书
- ✓ISO9001质量管理体系认证
- ✓多项产品通过了国家密码管理局的产品鉴定
- ✓已批准5项专利，多项专利在申请中
- ✓软件著作权40多项

公司产品和方案

- 终端安全产品
  - ✓USBKey、TF加密卡、手机盾
- 通信加密
  - ✓国密安全浏览器
  - ✓国密SSL 组件
- 数据安全
  - ✓数据库加密
- 安全解决方案
  - ✓国密安全接入系统
- 信创名录产品
  - ✓USBKey、安全浏览器、手机盾认证系统、数据库加密

手机盾

国密安全浏览器



密码产品目标

PART. 02

密码干什么

身份认证

你是谁？保证通信双方的身份是真实的，
在某些场景，可以只验证一方的身份。

完整性

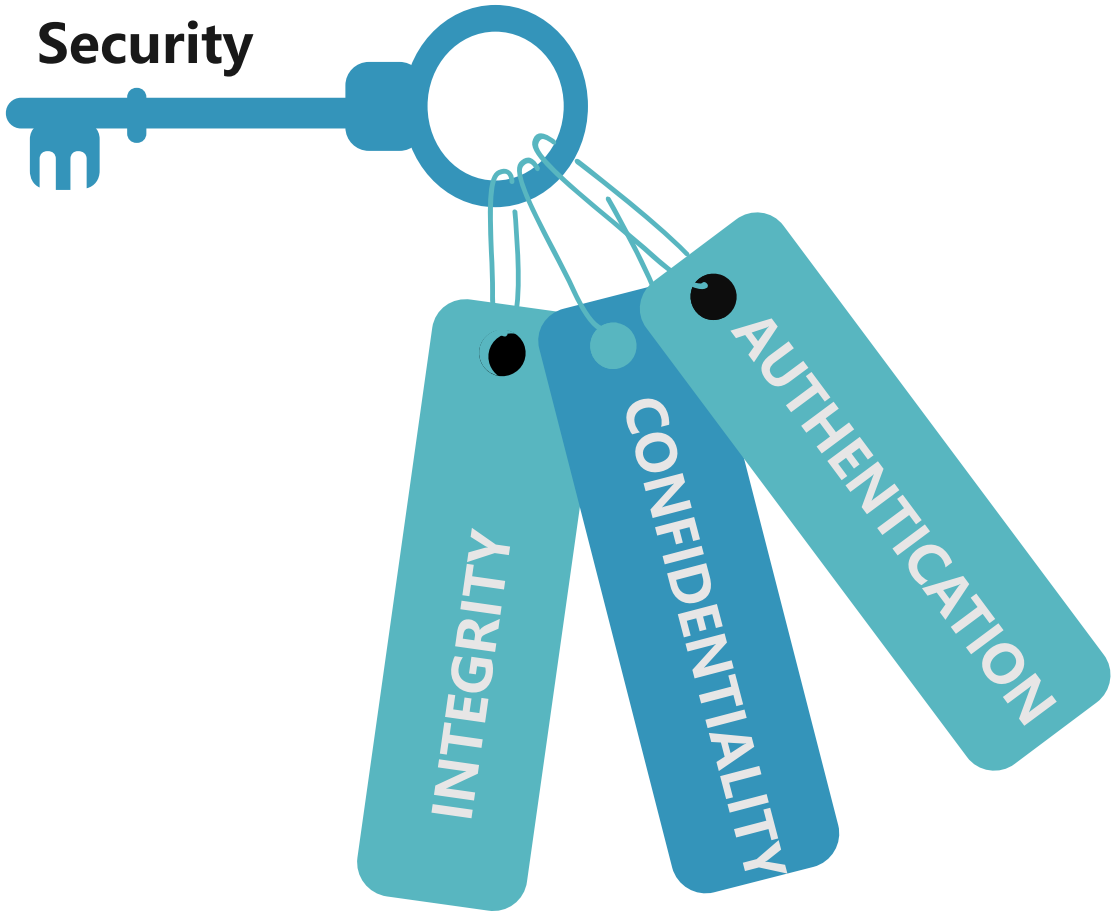
保证数据不能被篡改或删除。

机密性

机密性是指非法用户是不能窃取数据信息。

不可否认性（抗抵赖）

发送方对他发送的信息或是行为是不能否认的。

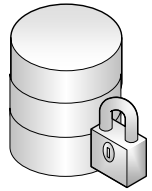


密码产品目标

- 认证
  - ✓USBKey、TF加密卡、手机盾
  - ✓动态令牌（OTP）
  - ✓签名验签服务器
- 通信加密
  - ✓国密安全浏览器、国密SSL 组件
  - ✓SSL VPN
  - ✓IPSec VPN
- 数据加密
  - ✓数据库加密
  - ✓密码机
- 关键行为的不可否认
  - ✓电子印章

手机盾

国密安全浏览器



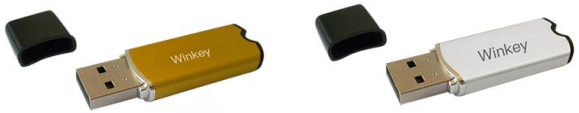
终端认证产品

PART. 03

UKey

智能密码钥匙

存储型智能密码钥匙



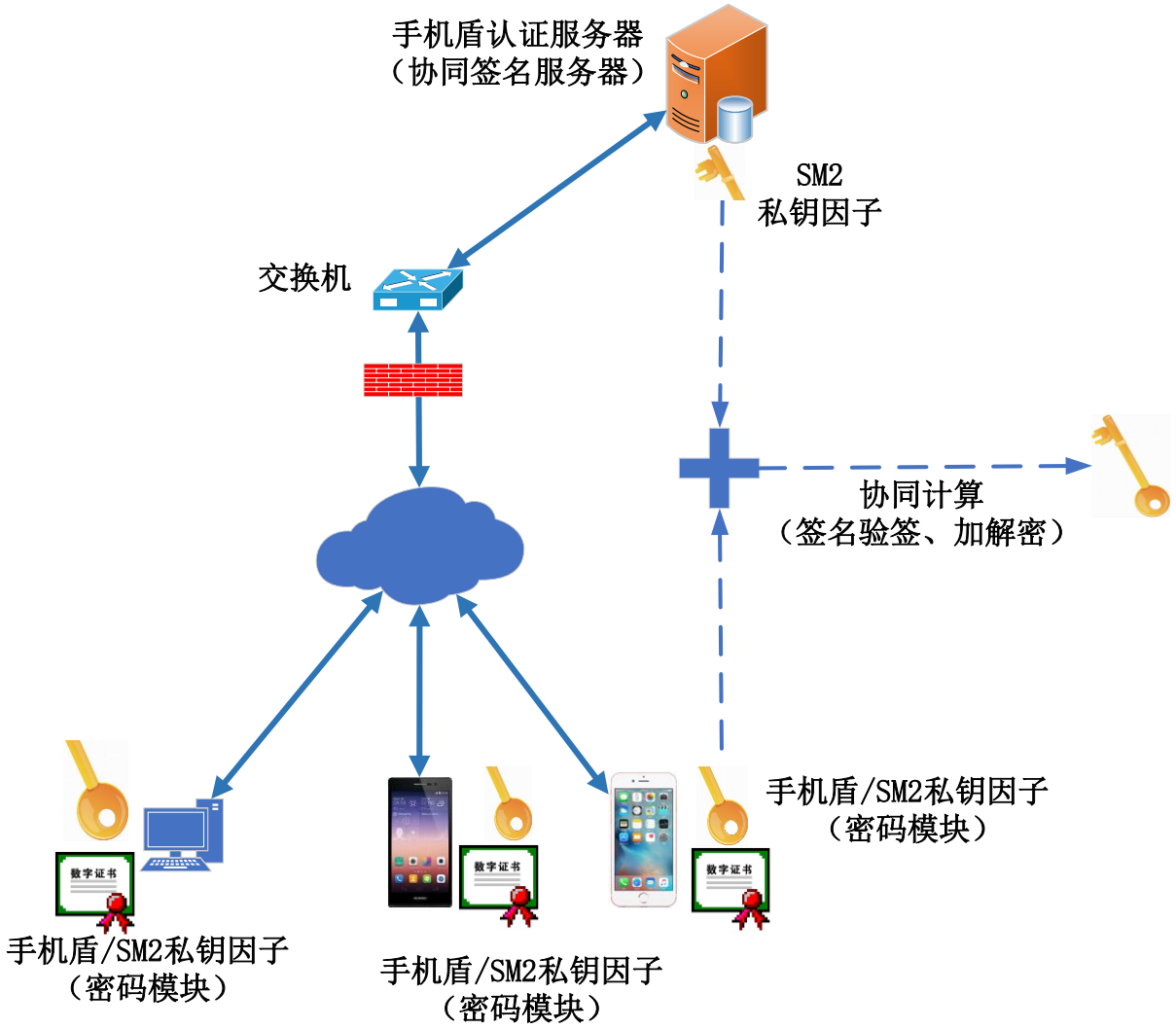
指纹Key

- 操作系统
  - Windows/Linux/国产操作系统
- 接口
  - SKF/ SOF
- 支持任意浏览器的任意版本
  - IE、Edge、Chrome、FireFox、国产浏览器、……
- 谁来验签?
  - 签名验签服务器
  - 配套应用

SD密码卡（TF密码卡）

- 主要用于移动端
  - Android PAD
  - 工控设备
  - 摄像头
  - ……
- UKey的另外一种形态
- 安全中间件
  - SKF国密接口

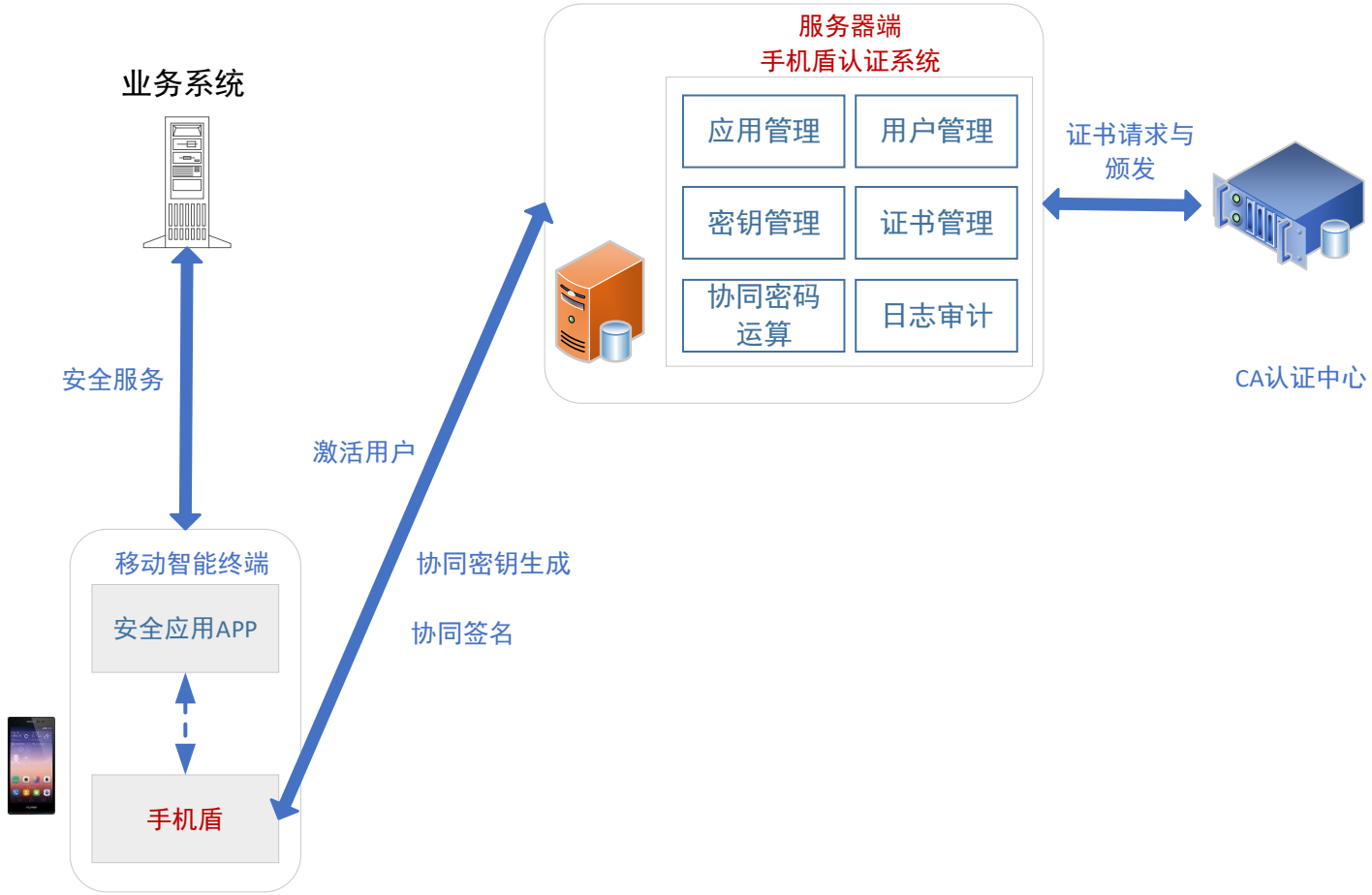
手机盾+手机盾认证系统——系统架构



- 密钥生成
  - 私钥分割、协同运算
  - 移动端、云端各自生成自己的密钥因子，在任何时间，任何一方无完整私钥
- 密钥使用
  - 移动端、云端各自进行自己的计算，按专利安全协议进行交互，完整私钥永不出现在内存中
- 操作系统支持
  - 支持Android、iOS、Windows、Linux等任意操作系统；
  - 支持小程序；
- 通道加密
  - 手机盾与手机盾云认证服务器之间采用国密SSL协议保护
- 便捷性
  - 无需任何终端硬件
- 安全性
  - “PIN+证书”双因子认证；

手机盾+手机盾认证系统——部署架构

- 手机盾认证系统支持本地化部署、云化部署
  - 仅要求IP可达
  - 无需与业务系统部署在同一个网段



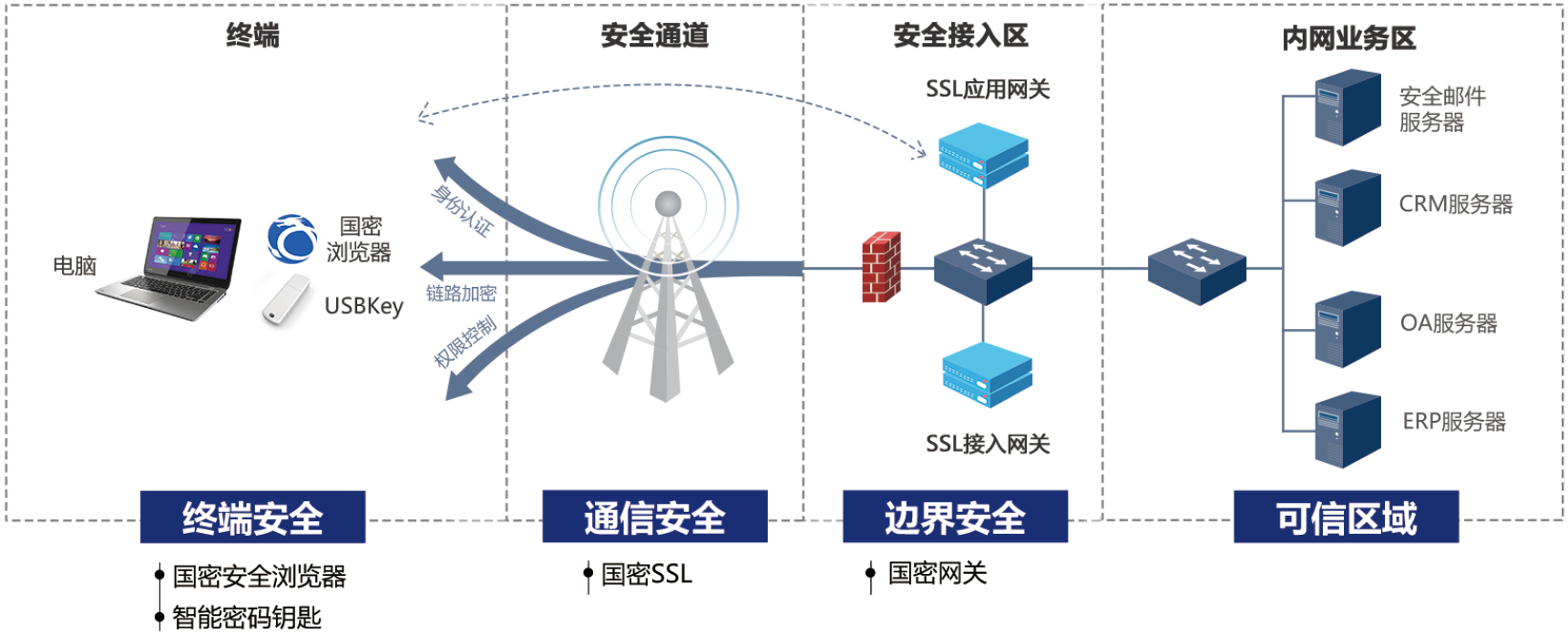
通道加密——国密浏览器、国密SSL组件

PART. 04

安全浏览器

基础功能

- 网页浏览
- HTTPS支持国密SSL协议，符合GM/T 0024-2012《SSL VPN技术规范》
- 与服务端SSL安全网关之间建立国密SSL通道
- 支持任意厂商UKey



安全浏览器

增强功能

- 双核支持，按应用指定内核
- NPAPI支持
- Flash支持
- XP支持
- 环境检测与一键修复
- 保密管控

Blink内核 | IE内核

支持

支持

延续NPAPI支持

延续Flash支持

- Chrome 69版开始，逐步限制使用Flash插件，即便允许某个站点的flash播放
- Chrome 50 …的支持；

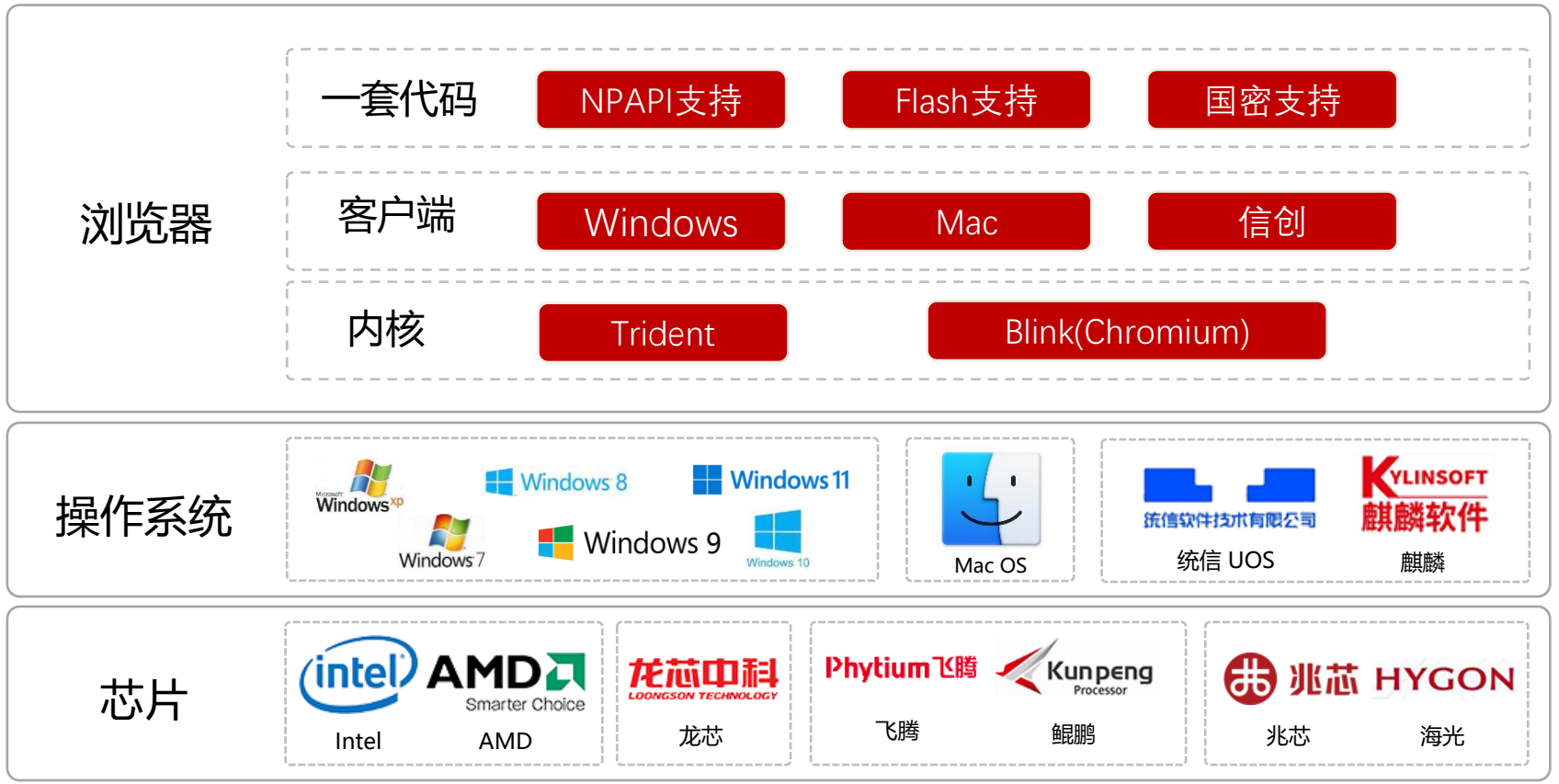
系统环境安全

一键安装 | 系统环境检测

服务管理端

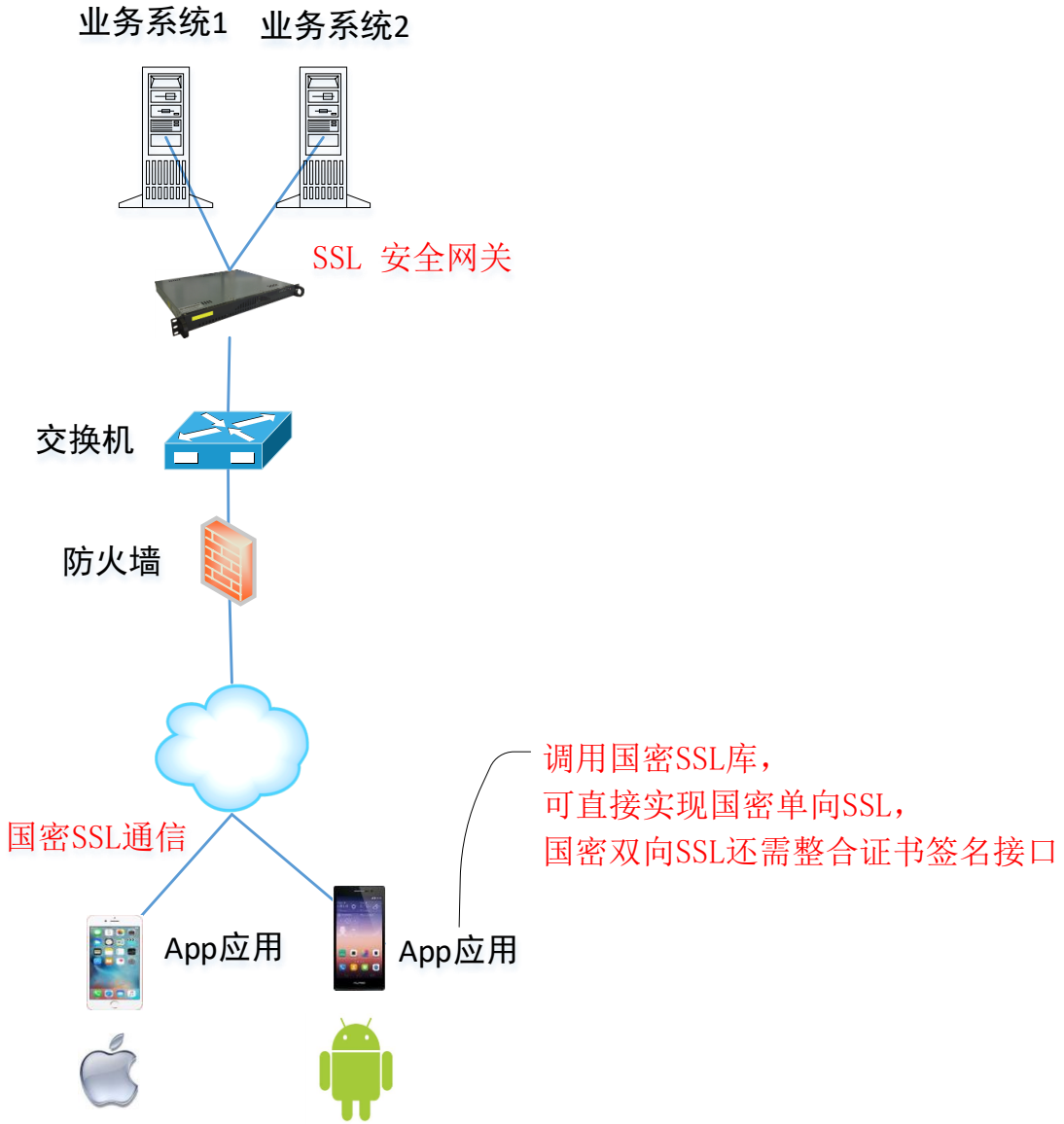
策略管理	授权管理	日志管理	配置管理	权限管理	功能管理
策略管理	授权设备	操作日志	第三方配置	后台用户列表	禁止地址栏
受信任站点管理	用户管理	崩溃日志	系统配置	后台用户角色	禁止拖拽
应用管理	角色管理	设备日志		后台用户菜单	禁止右键菜单
允许弹出窗口管理		错误日志		后台用户角色	禁止另存为
内核管理					禁止打印
证书选项管理					禁止复制&黏贴
插件管理					禁止源代码
IE选项管理					
屏蔽网站管理管理					

安全浏览器


浏览器
一套代码
NPAPI支持
Flash支持
国密支持
客户端
Windows
Mac
信创
内核
Trident
Blink(Chromium)
操作系统
Windows xp
Windows 8
Windows 11
Windows 7
Windows 9
Windows 10
Mac OS
统信软件技术有限公司
KYLINSOFT
麒麟软件
统信 UOS
麒麟
芯片
intel
AMD
Smarter Choice
Intel
AMD
龙芯中科
LOONGSON TECHNOLOGY
龙芯
Phytium飞腾
Kunpeng
Processor
飞腾
鲲鹏
兆芯
HYGON
兆芯
海光

国密SSL组件

- 国密SSL网络库（WTGMNet）
  - 实现国密SSL协议的网络架构，支持单双向国密SSL协议
  - 兼容Android、iOS
  - SDK只需增加3-5M
  - 支持原生调用
  - 无需修改原有App架构
    - ✓ 支持WebView、WKwebView、UIwebView、H5调用
    - ✓ 支持Android OKHttp、httpClient，iOS AFNetworking / NSURLConnection/NSURLSession网络框架
- 简便接入
  - 只需App初始化时简单配置，其它代码无需修改
  - 工作量：大约200行代码
- 可与手机盾整合成一个SDK



国密SSL组件

- 国密SSL网络库（Java接口）
  - 提供基于Java的接口
  - 提供基于Socket的国密SSL协议接口封装，支持服务器端、客户端调用
  - 提供基于https的国密SSL协议接口封装
  - 符合BouncyCastle 架构，易于集成调用
  - 提供定制接口开发服务
  - 支持JDK 1.6以上

国密SSL组件

- 国密SSL组件与VPN SDK的区别
  - 不同厂商的VPN SDK不能互通
  - 国密SSL 组件支持任意厂商的SSL VPN 网关（反向代理模式）

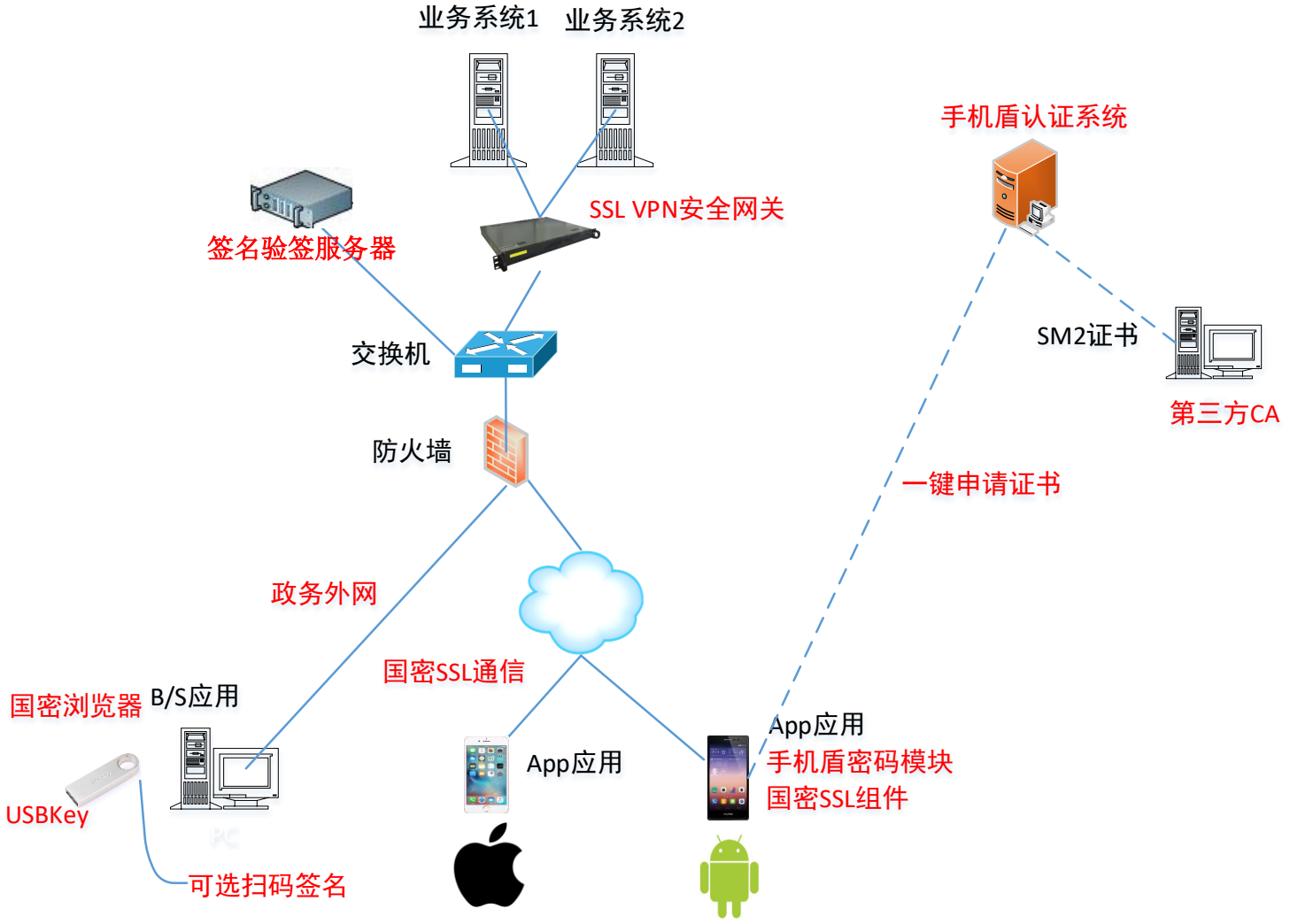
- VPN 网关的分类与应用
  - SSL 安全认证网关
    - ✓ 自定义协议的认证
    - ✓ 仅限于部分政企内部应用
    - ✓ 利旧项目，极难支持
  - SSL 应用网关（SSL卸载网关）
    - ✓ 反向代理模式
    - ✓ 只做通道加密
    - ✓ 面向大规模公众服务只能使用SSL应用网关
    - ✓ 容易对接
    - ✓ 推荐使用

国密安全接入系统

PART. 05

国密安全接入系统

- 国密安全接入系统
  - 通道安全
    - ✓ 安全应用网关（反向代理模式，网关只做SSL通道，不做认证，认证由应用层来做，客户端不需要VPN厂商SDK）
    - ✓ 手机盾，内嵌国密SSL组件
    - ✓ 国密浏览器
  - 认证
    - ✓ 签名验签服务器（密码机）
    - ✓ 手机盾+手机盾认证系统
      - 支持Android、iOS、Windows、Linux等任意操作系统；
      - 支持小程序；
    - ✓ USBKey
  - 证书服务
- 特点
  - 安全应用网关、国密浏览器、国密SSL组件做通道安全
  - 签名验签服务器、USBKey 、手机盾做认证



国密安全接入系统——方案优势

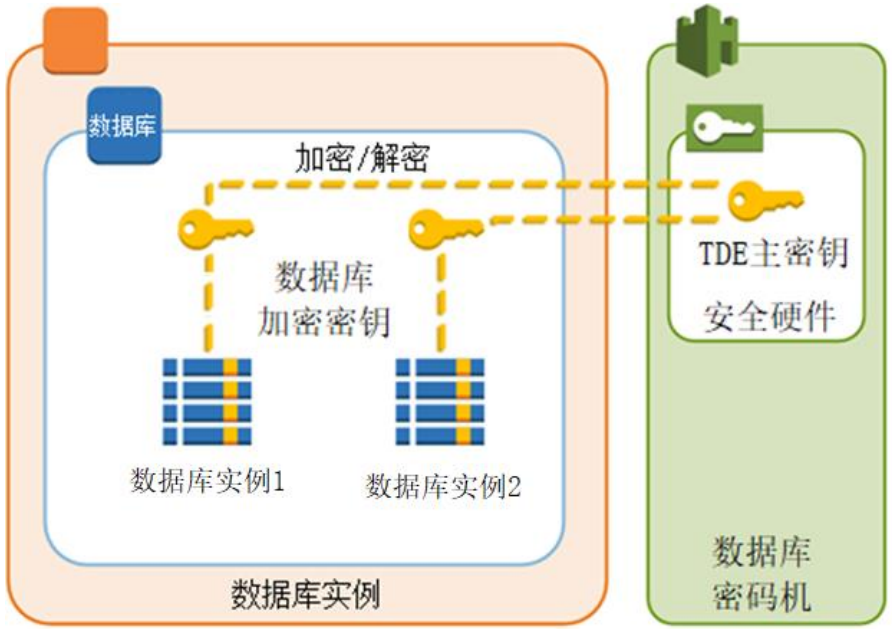
协调、对接工作量少，可保证快速上线

	传统方案 （VPN网关采用认证模式）	本方案 （VPN网关采用反向代理模式）
PC端	1）需要VPN网关与业务系统实现单点登录； 2）需要业务系统对接 UKey；	1）只需业务系统对接 UKey； 2）对接工作量不超过1周；
移动端	1）需要VPN 客户端SDK与手机盾SDK整合，再提供给App厂商整合； 2）一个App/操作系统的对接工作量大约3个月；	1）无需VPN厂商SDK； 2）一个App/操作系统的对接工作量大约3周；
对VPN网关厂商要求	需要VPN网关厂商动用研发，做大量技术支持	只需VPN网关配置成反向代理，零技术支持
结论	1）需要VPN网关厂商、业务系统开发商、手机盾厂商、UKey厂商做多家的应用对接； 2）协调工作量极大，项目进度难以保证；	1）与传统方案对比，本方案减少业务系统开发商3个月的对接工作量，且基本上无需VPN网关厂商做技术支持； 2）我司实现全部技术支持，可保证快速上线；

数据库加密

PART. 06

数据库加密——透明加密



- 优点
  - 透明加密 (TDE， Transparent Data Encryption)
    - ✓ 存储加密，支持完整性保护
    - ✓ 授权用户/应用为明文
    - ✓ 应用无需做任何改造
  - 支持所有关系型数据库
    - ✓ 包括但不限于MySQL、MariaDB、Postgre、SQLServer、Oracle、DB2、Informix、达梦、南大通用、神通、人大金仓等数据库
  - 支持数据库的所有功能和语法
  - 一台数据库密码机，支持多个数据库实例
  - 加密密钥独立于数据库数据，存储在数据库密码机中

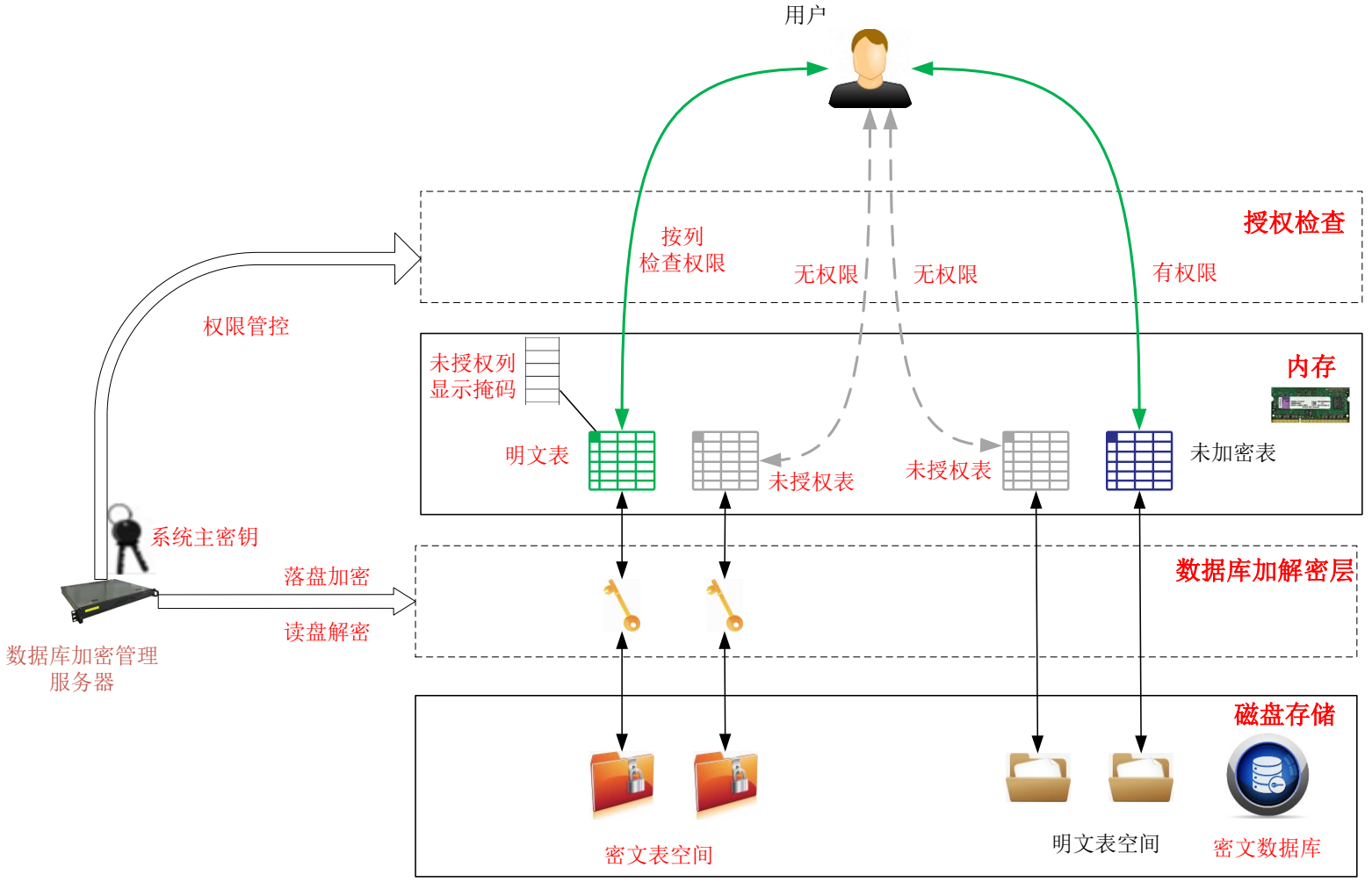
数据库加密——表加密

支持数据库类型

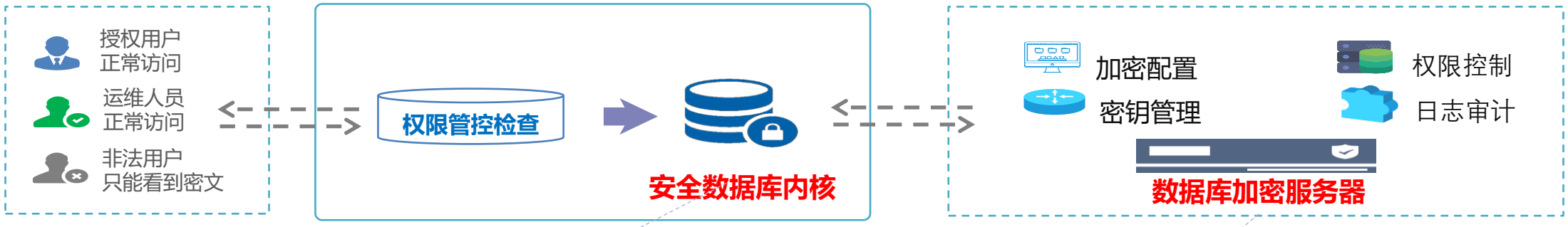
- MySQL（5.7及以上）
- MariaDB （ 10.3.7及以上）

核心功能

- 全透明加密，支持所有SQL语法。
- 扩展内核引擎，改造 MySQL InnoDB / MariaDB Maria 存储引擎，实现在存储层的加解密功能。实现加密保护的同时，保证 MySQL/MariaDB的原有其它功能与性能。
- 具备权限管控功能。



数据库加密——表加密



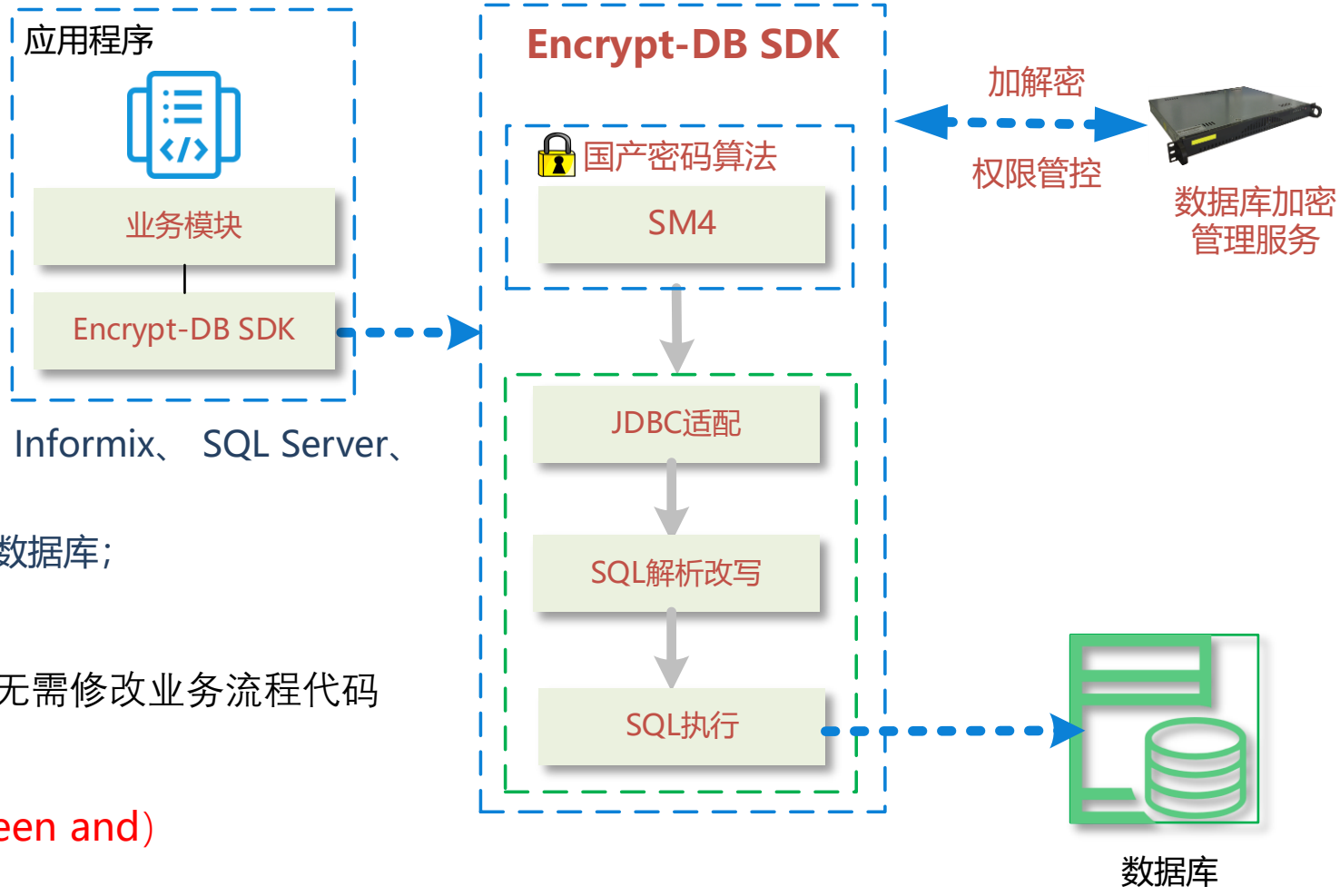
安全数据库内核：

- 内置加密插件，数据库内核级加密
- 业务系统零修改
- 支持任意SQL语法
- 兼容第三方数据库运维工具
- 整合性能下降<2%
- 支持存储过程、触发器、视图

健壮性：

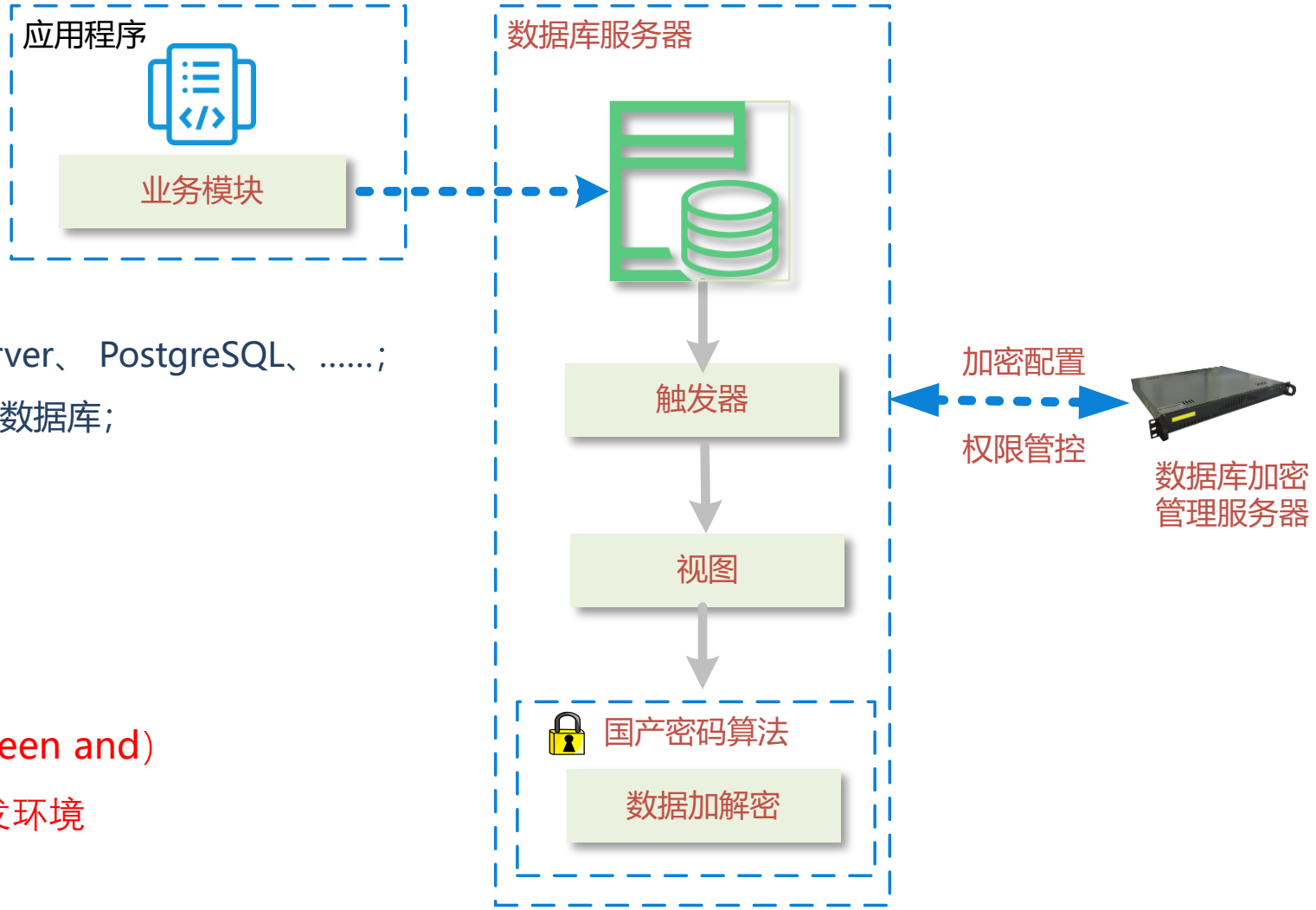
- 数据库加密机重启、数据库服务器重启、应用服务器重启不影响数据库加密的运行

数据库加密——应用系统侧列加密



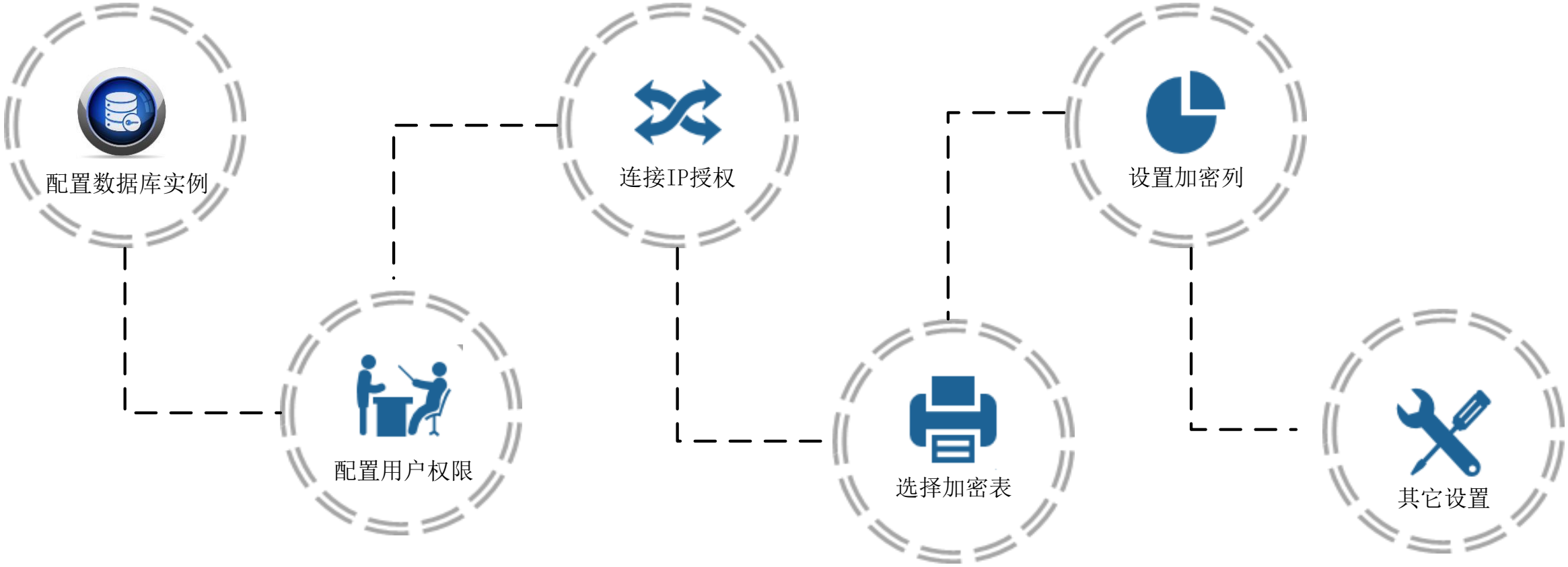
- 支持数据库
  - MySQL、MariaDB、Oracle、DB2、Informix、 SQL Server、PostgreSQL、……;
  - 达梦、神通、南大通用、金仓等国产数据库;
- SM4加密、HMac（基于SM3）完整性
- 提供Encrypt-DB SDK，需要重新编译，无需修改业务流程代码
- 支持密文的模糊查询（like）
- 支持密文的数值比较（<、>、=、between and）
- 应用服务器要求为Java环境

数据库加密——数据库侧列加密



- 支持数据库
  - Oracle、DB2、Informix、 SQL Server、 PostgreSQL、……;
  - 达梦、神通、南大通用、金仓等国产数据库;
- SM4加密、HMac（基于SM3）完整性
- 无需修改应用代码
- 数据库服务器安装触发器、视图
- 支持密文的模糊查询（like）
- 支持密文的数值比较（<、>、=、between and）
- 对应用服务器无任何要求，支持任意开发环境

数据库加密——使用配置



数据库加密——UI展示

数据源名称： 请输入数据源名称　　IP地址： 请输入IP地址

数据源名称	IP地址	连接端口
mysql	192.168.199.132	3306
test	192.168.199.190	3312
testaa	192.168.199.190	3306

数据源： mysql　　数据库： test1　　* 数据表： user

加密器： 请选择加密器　　加密算法： 请选择加密算法　　加密状态： 请选择　　搜索

刷新列表　　执行任务

列名	加密器	加密算法	加密状态	执行状态
id				
username	请选择加密器		未加密	
password	请选择加密器		未加密	
avatar	请选择加密器		未加密	
phone	请选择加密器		未加密	
email	请选择加密器		未加密	
disabled	请选择加密器		未加密	

数据库加密——产品优势

- ✓ 机密性：SM4
- ✓ 完整性：基于SM3的HMac
- ✓ 支持所有关系型数据库
  - ➢ 包括但不限于MySQL、MariaDB、Postgre、SQLServer、Oracle、DB2、Informix、达梦、南大通用、神通、人大金仓等数据库

- ✓ 表加密：效率下降小于2%
- ✓ 列加密：
  - ➢ 未加密列无影响
  - ➢ 精准查询（通过明文列查询密文列数据），下降5%以内
  - ➢ 密文列的模糊查询时效率下降15%

- ✓ 授权用户操作透明
- ✓ 应用操作透明
- ✓ 兼容数据库常用的运维工具和手段
- ✓ SQL 语法全兼容
- ✓ 原有应用无需改造
- ✓ 业务系统只需配合测试
- ✓ 可视化UI操作，易用性好

- ✓ 双机热备
- ✓ 密钥独立存储，保证加密文件可恢复
- ✓ 提供离线密钥恢复工具，提供加密备份、导入工具
- ✓ 数据库重启、业务系统重启、数据库密码机重启无影响

数据库加密——方案对比

- 密码机加密
  - ✓ 提供SDF库（加密SDK ）
  - ✓ 应用需要大规模改造，业务系统开发人员不了解密码接口应用，需要大量技术支持
  - ✓ 沟通成本高昂
  - ✓ 一旦需求变更，需要重新开发
  - ✓ 不支持模糊查询

- 数据库透明加密
  - ✓ 原有应用无需改造
  - ✓ 在第三方应用获得授权的前提下，支持第三方应用合法导出数据；
  - ✓ 业务系统只需配合测试
  - ✓ 可灵活配置加密表、加密列
  - ✓ 快速实施

政务密改方案

PART. 07

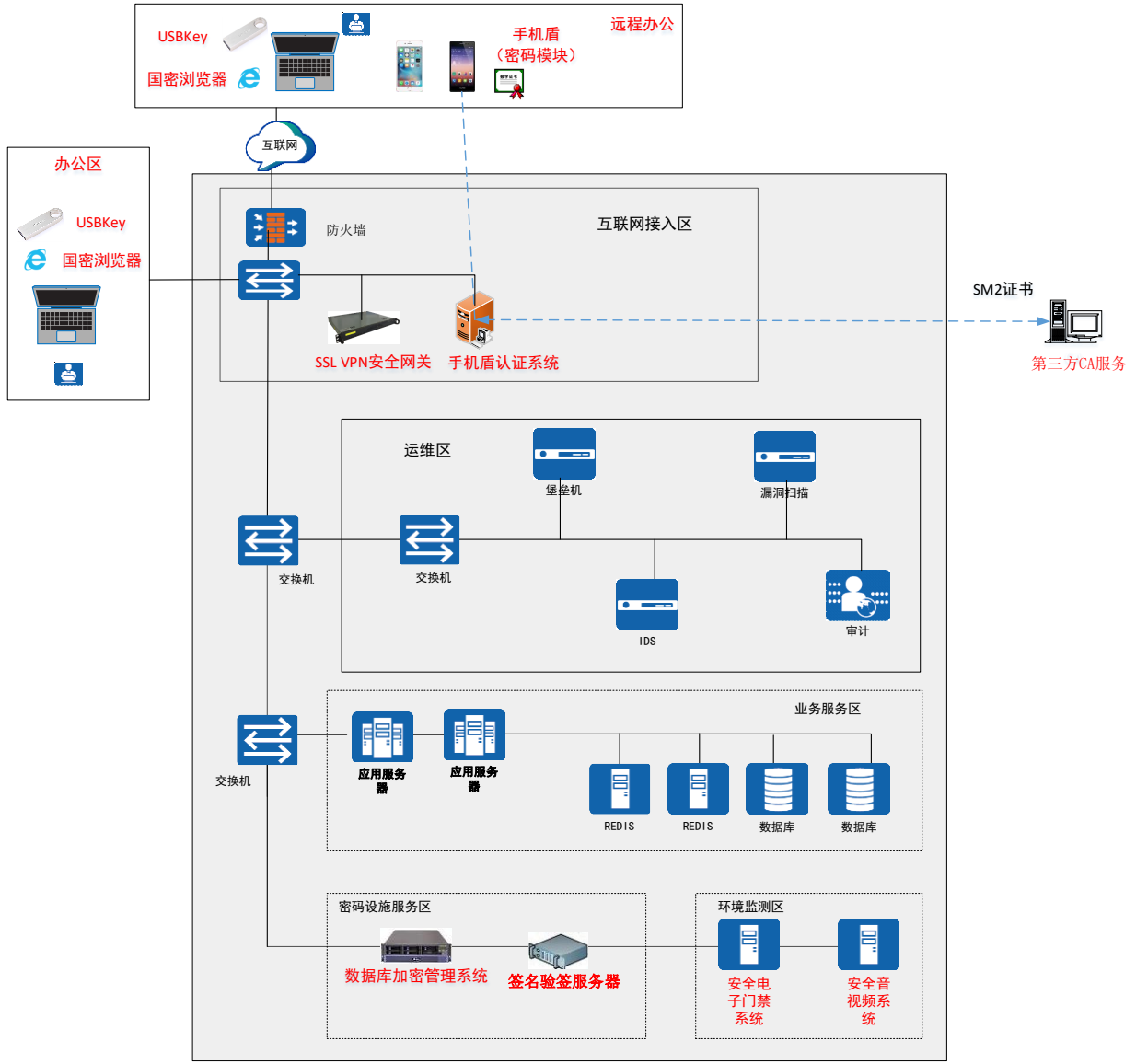
政务密改方案

- 国密安全接入
  - 通道加密
  - 业务系统身份认证
- 数据库加密
  - 业务系统数据存储安全
- 辅助软件
- 门禁和视频监控

政务密改方案——密码设备/软件清单

序号	产品名称	部署位置	使用的密码算法	数量	用途
1	SSL VPN安全网关	网络接入区	SM2/3/4	2台	1）实现业务和数据安全中的远程安全接入，在PC到服务器端建立国密安全传输通道； 2）同时实现网络和通信安全中的传输通道安全； 3）同时实现设备和计算安全中的集中管理通道安全；
2	浏览器密码模块	业务办公区	SM2/3/4	按需配置	1）在业务和数据安全中，在PC到服务器端建立国密安全传输通道； 2）同时实现网络和通信安全中的传输通道安全； 3）同时实现设备和计算安全中的集中管理通道安全；
3	USBKey	业务办公区； 统一管理区	SM2/3/4	按需配置	1）最终用户远程登录业务系统； 2）管理员登录业务服务管理端；
4	手机盾密码模块	移动终端	SM2/3/4	按需配置	1）内置国密SSL组件，实现移动端与VPN网关之间的国密SSL安全通道 2）与手机盾认证系统配合工作，实现移动端用户远程安全接入的身份鉴别
5	手机盾认证系统	网络接入区	SM2/3/4	2台	与手机盾密码模块配合，实现移动端用户远程安全接入身份鉴别
6	数据库加密管理系统	业务服务区	SM3/4	2台	实现业务数据中敏感数据的加密存储，完整性保护
7	密码机/签名验签服务器	业务服务区	SM2/3	2台	与应用服务管理系统配合，实现签名、验签，保证业务系统行为的不可否认性，以及系统日志的完备性、重要程序或文件完整性，
8	应用服务管理系统	业务服务区	SM2/3	-	配套软件 与签名验签服务器配合，实现签名、验签，保证业务系统行为的不可否认性，以及系统日志的完备性重要程序或文件完整性，
9	证书服务	-	SM2/3	按需配置	采用第三方 CA的证书服务

政务密改方案——密码应用部署

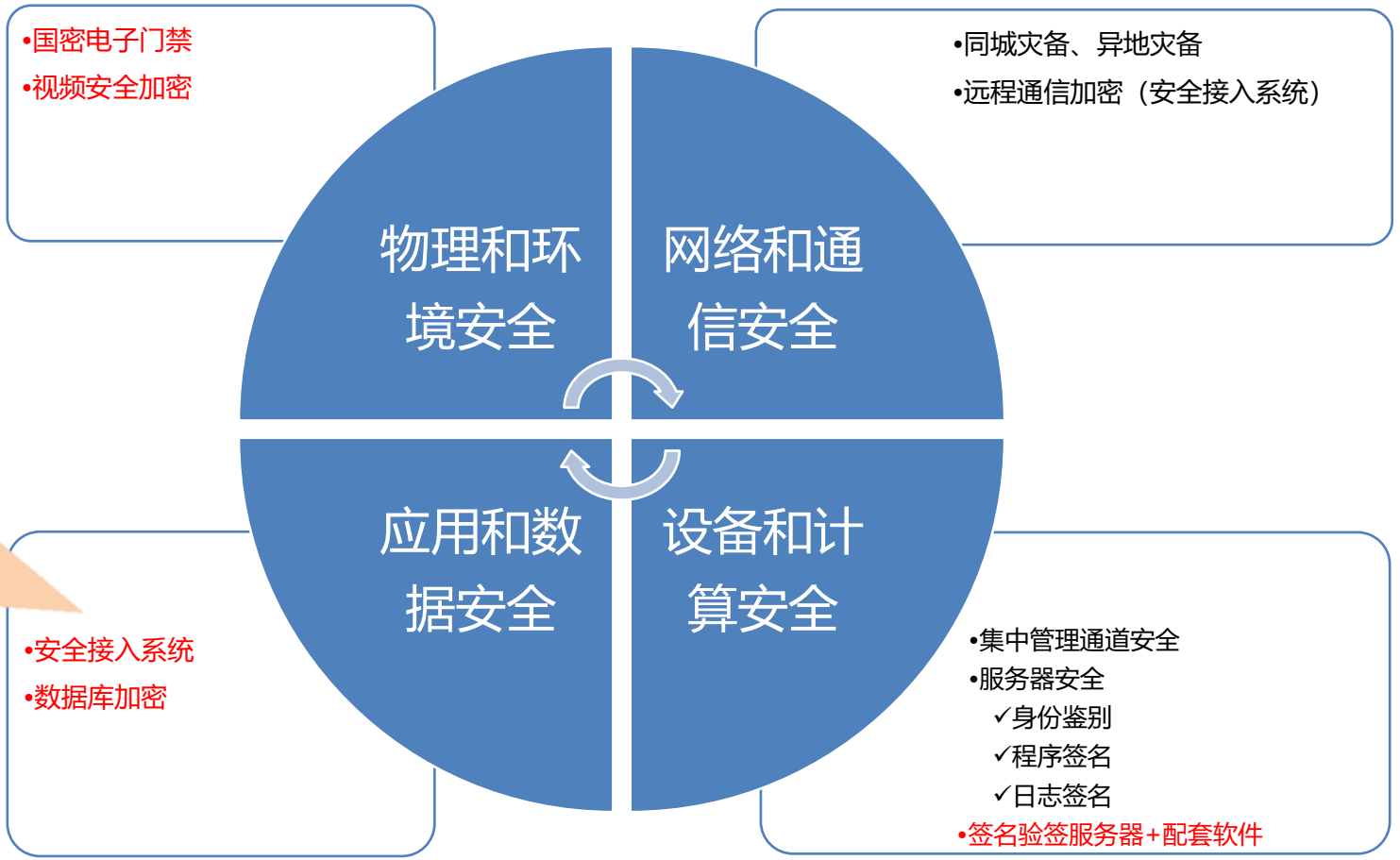


政务密评应对

PART. 07

密评应对

- 安全接入
  - 网络通信加密
  - 身份认证
  - 支持PC、移动端
- 数据库安全
  - 数据完整性
  - 数据存储加密
    - ✓ 透明加密，无需业务系统修改代码
    - ✓ 支持任意关系型数据库



满足密码测评要求

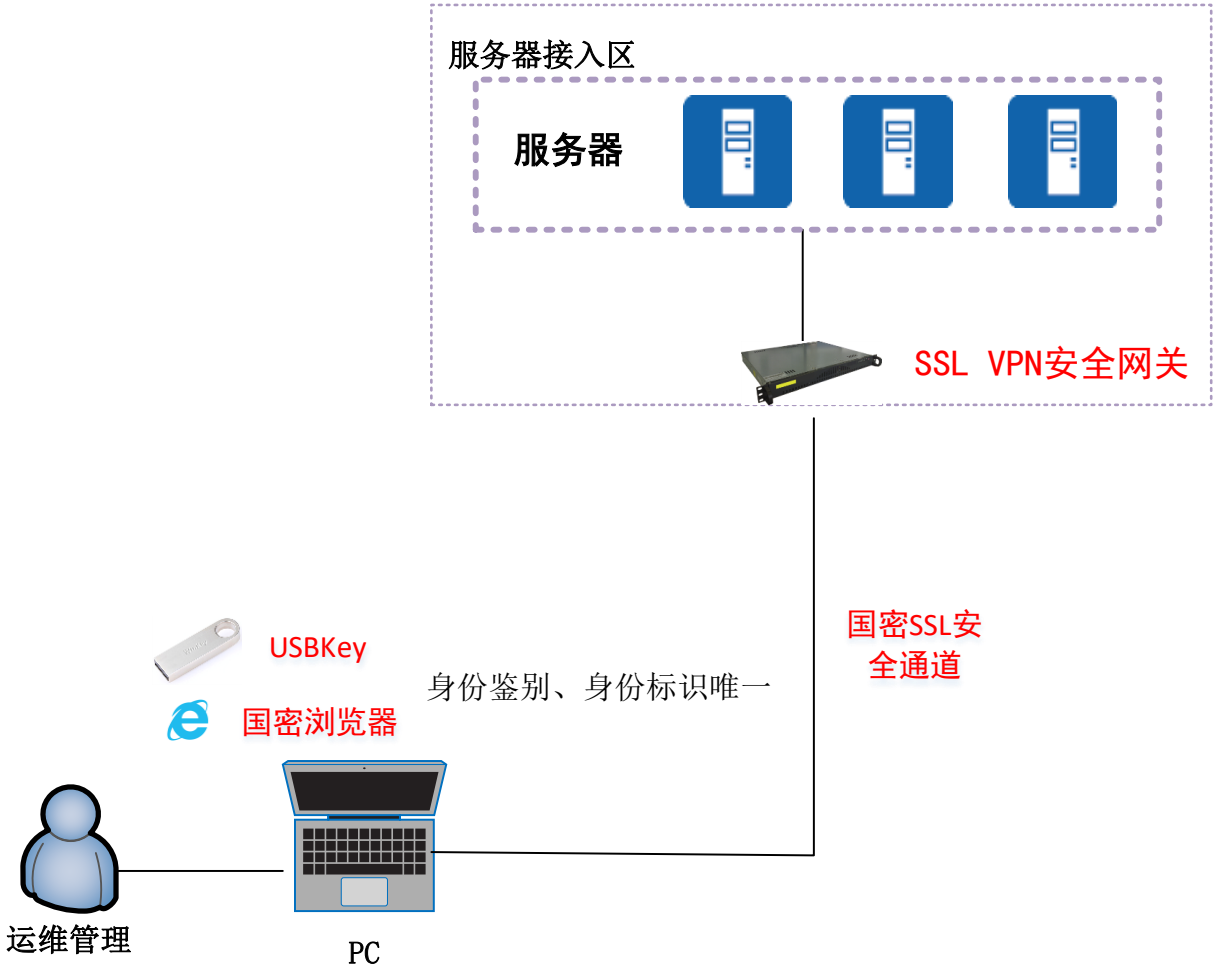
从到网络和通信安全（安全集中管理）、到设备和计算安全（程序签名、日志签名）、应用和数据安全（安全接入、数据库加密）、以及物理和环境安全（电子门禁、视频监控）的全方位安全；

网络和通信安全

- 检查要点
  - 网络和通信安全层面的认证，只需要认证服务器，即服务器端部署SSL网关，部署SSL服务器证书即可
- 同城灾备、异地灾备
  - IPSec网关，实现数据备份
- 远程访问的网络通信安全
  - 国密安全接入系统
    - ✓ SSL VPN安全网关
    - ✓ 国密浏览器
    - ✓ USBKey
    - ✓ 手机盾密码模块
    - ✓ 手机盾认证服务器
    - ✓ 证书服务

设备和计算安全

- 检查要点
  - 身份鉴别、集中管理通道安全
    - ✓ SSL VPN安全网关
    - ✓ 国密浏览器
    - ✓ USBKey
  - 完整性（重要应用、日志）
    - ✓ 签名验签服务器
    - ✓ 应用服务管理系统（配套软件）



应用和数据安全

检查要点

- 通道加密、存储加密、身份认证

政企办公应用

- 国密安全接入系统（与网络与通信安全的通道加密有重复）
  - ✓ SSL VPN安全网关
  - ✓ 国密浏览器
  - ✓ USBKey
  - ✓ 手机盾+手机盾认证服务器
  - ✓ 证书服务

数据存储机密性、完整性

- 数据库加密管理系统

感谢倾听！

天津市商用密码行业协会