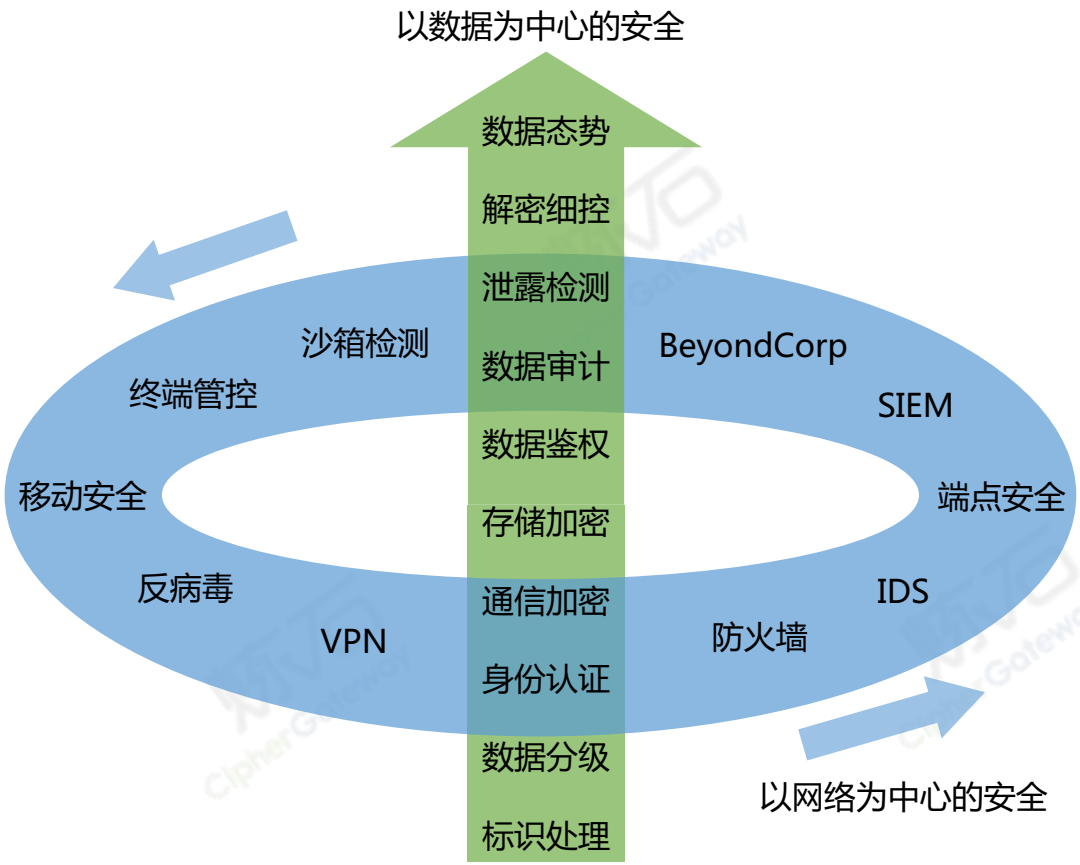
炼石
CipherGateway

图解22种密码应用模式

炼石网络CEO 白小勇

1 密码应用创新迫在眉睫

安全需求演进、国密政策出台，推动密码复兴



双轴驱动的新安全建设体系

2018年2月【密码监管抓手】密评试点

- 首批商用密码应用安全性测评机构资质下发，**并针对甲方单位开展商用密码应用安全性评估试点工作。**
- **2019年会达到约50家密评单位。**

2018年7月【政策强推】两办XX号文

- 明确各大部委和地方政府国密推广相关任务
- 财政配套国密应用推广专项资金

2019年5月【抓手增强】公安部《等级保护条例2.0》

- 8.1.2.2 应采用密码技术**保证通信过程**中数据的完整性、保密性
- 8.1.4.7 应采用密码技术**保证重要数据在传输、存储过程**中的完整性
- 8.1.4.8 应采用密码技术保证重要数据在传输、存储过程中的保密性
- 8.1.10.9 应使用**国家密码管理主管部门认证核准**的密码技术和产品

2019年6月【法律威慑】全国人大审议《密码法》

- 第八条 **县级以上人民政府**应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级预算。
- 第十二条 **关键信息基础设施**应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，**同步规划、 同步建设、同步运行密码保障系统**
- **第三十二条 违反本法第十条、第十二条规定使用密码的，由密码管理部门责令改正或者停止违法行为，给予警告；情节严重的，由有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。**
- **第四十条 违反本法规定，构成犯罪的，依法追究刑事责任。**

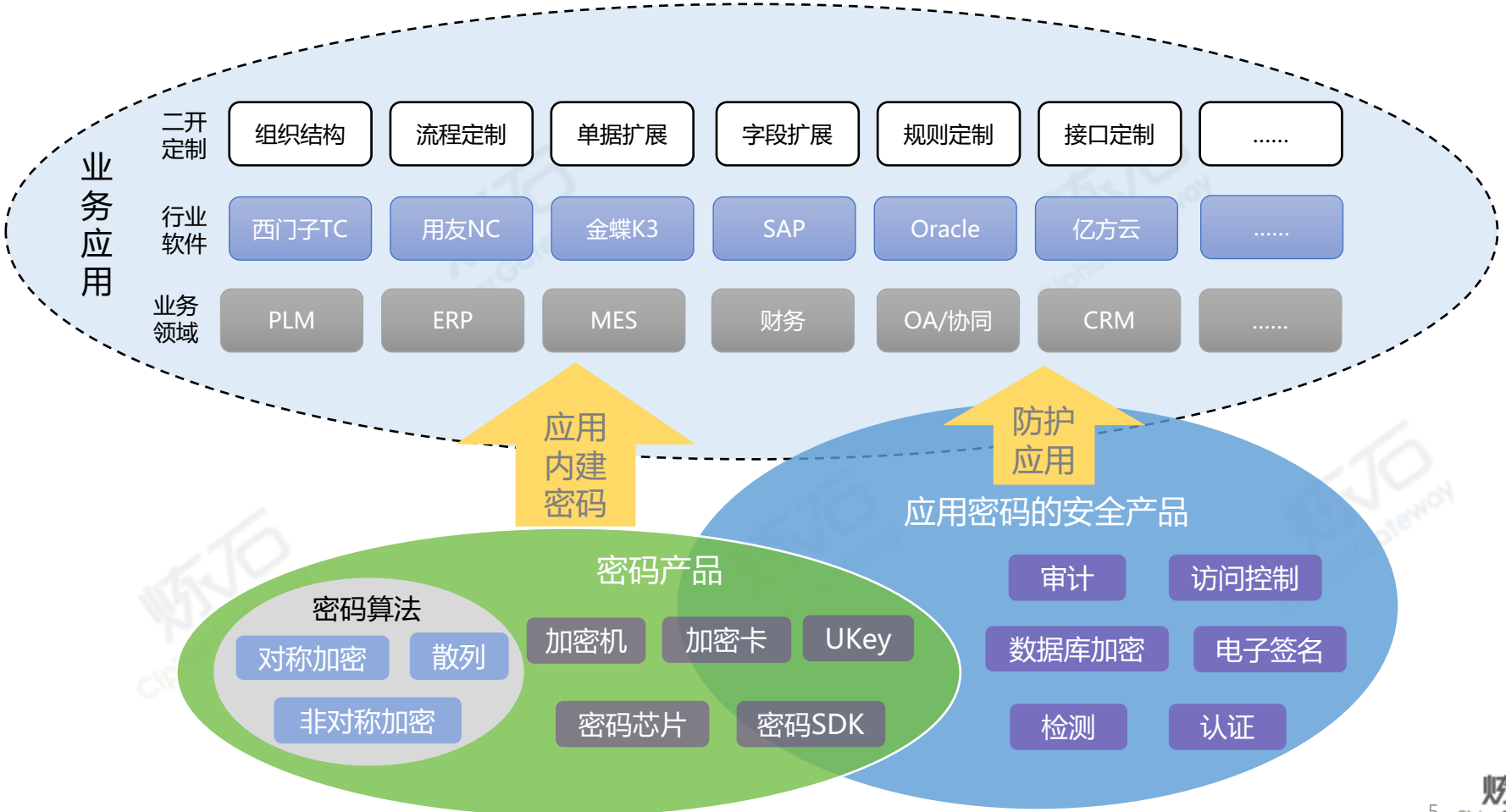
数据安全和国密整改两大需求场景呼唤密码创新

数据安全密码防护体系

* GM/T 0054-2018三级

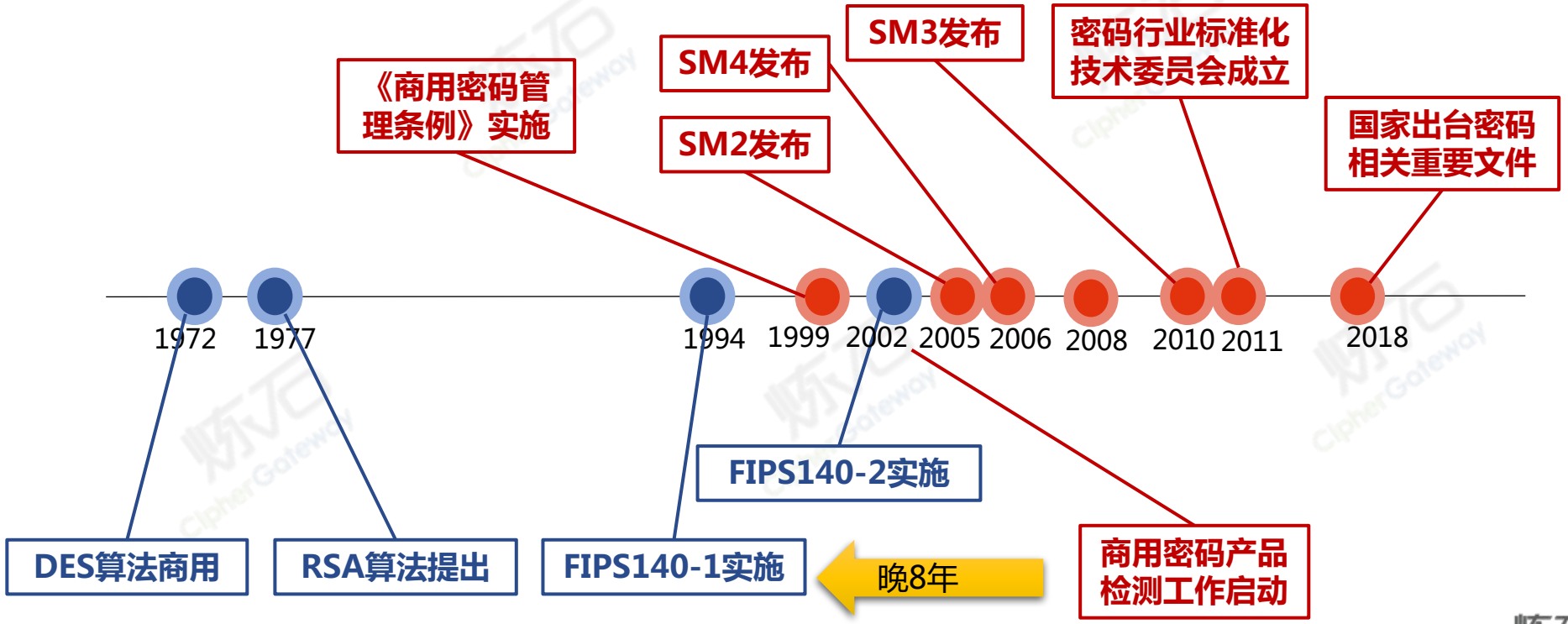
应用要求内容	炼石产品应用
a)应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；	炼石CipherSuite可与重要信息系统集成，提供内建的国密能力，辅助身份认证，保护数据在传输态、存储态的安全性； 炼石CASB可在不改造原有系统的前提下，为系统补足缺失的国密能力，保护数据在传输态、存储态的安全性，提供基于ABAC的动态访问控制，并提供第三方防篡改的日志审计； 炼石KLM提供必要的密钥管理功能。
b)应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；	
c)应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；	
d)应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；	
e)应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；	
f)应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等；	
g)应使用密码技术的完整性功能来实现对日志记录完整性的保护；	
h)应采用密码技术对重要应用程序的加载和卸载进行安全控制；	
i)宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。	

密码产业包含密码算法、密码产品、密码应用等环节



我国密码体系起步晚于美国，但可借鉴先进经验

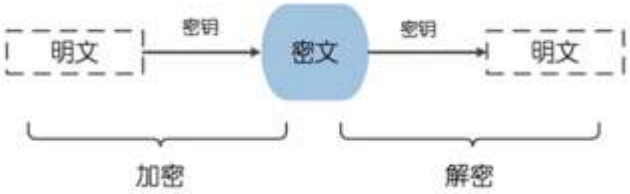
我国密码算法研制跟国际密码算法研制水平相当，
但密码产业特别是在密码应用方面存在近20年差距



中国自主密码算法已进入国际标准

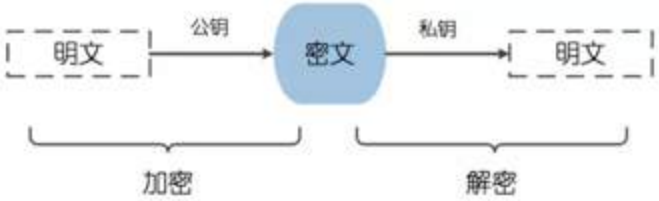
对称加密算法

- 中国商用密码：SM4(2012年发布,推荐)/SM1
- 美国：AES/3DES(开始弃用)/DES(已弃用)



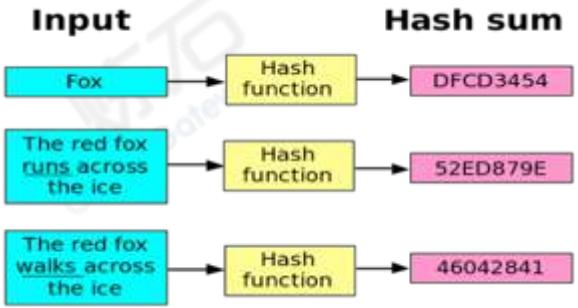
非对称加密算法

- 中国商用密码：SM2(2010年发布)/SM9
- 美国：RSA/ECC



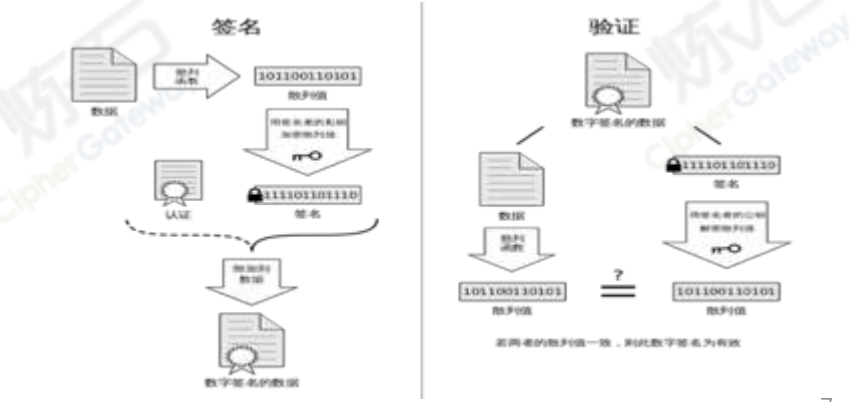
散列/杂凑/哈希算法

- 中国商用密码：SM3(2010年发布)
- 美国：SHA-3/SHA256/MD5(已弃用)



密码算法组合使用

- 数据签名验证场景



结合FIPS浅析中美密码产品差距及现存挑战

差距一

高性能需求与低效算法实现性能的矛盾

差距二

密码软件或混合形态少，难以覆盖云、移动端、IoT等新场景

差距三

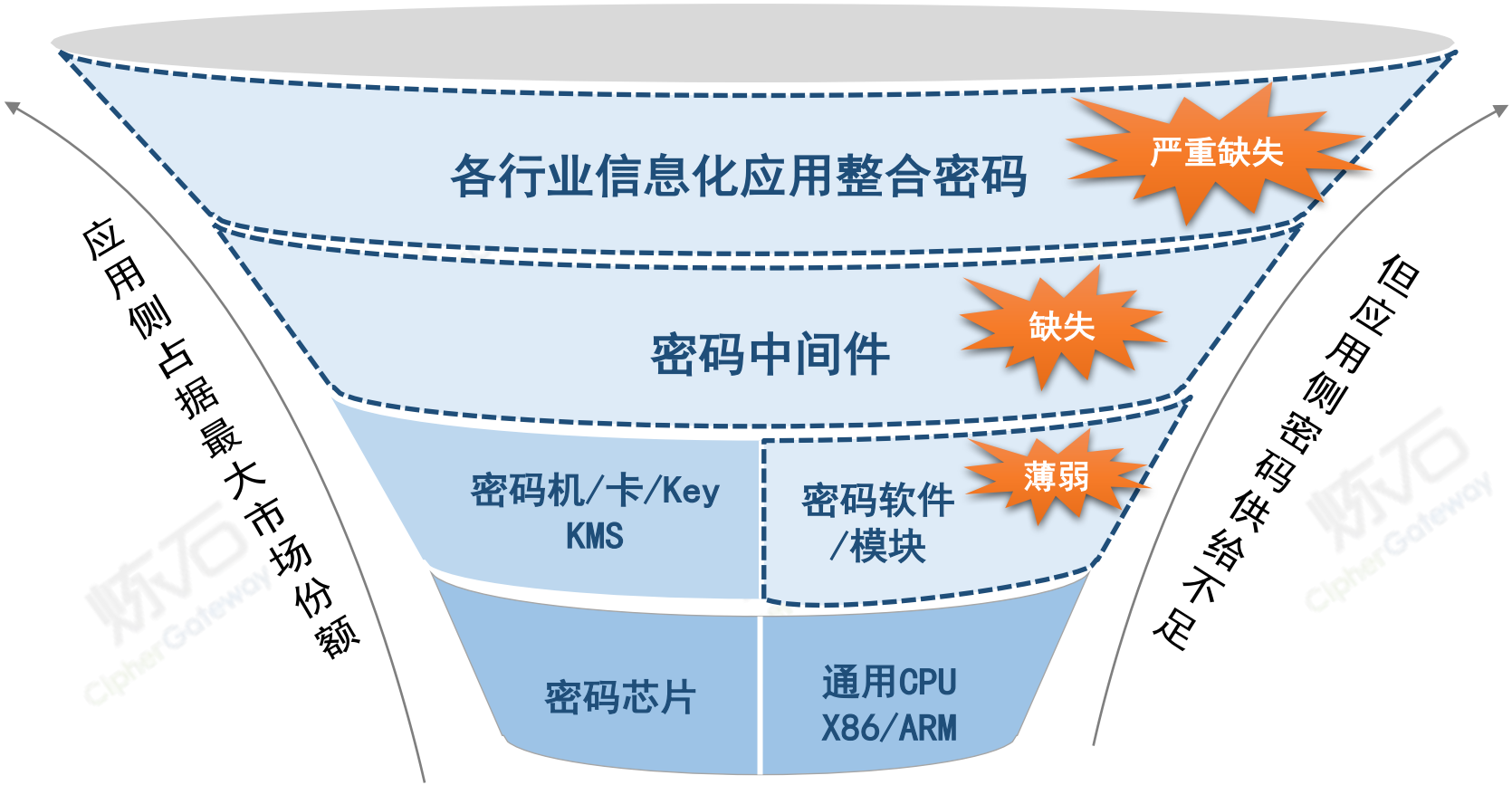
密码中间件缺失导致代码难以复用，同时开发商使用门槛极高

产业现状

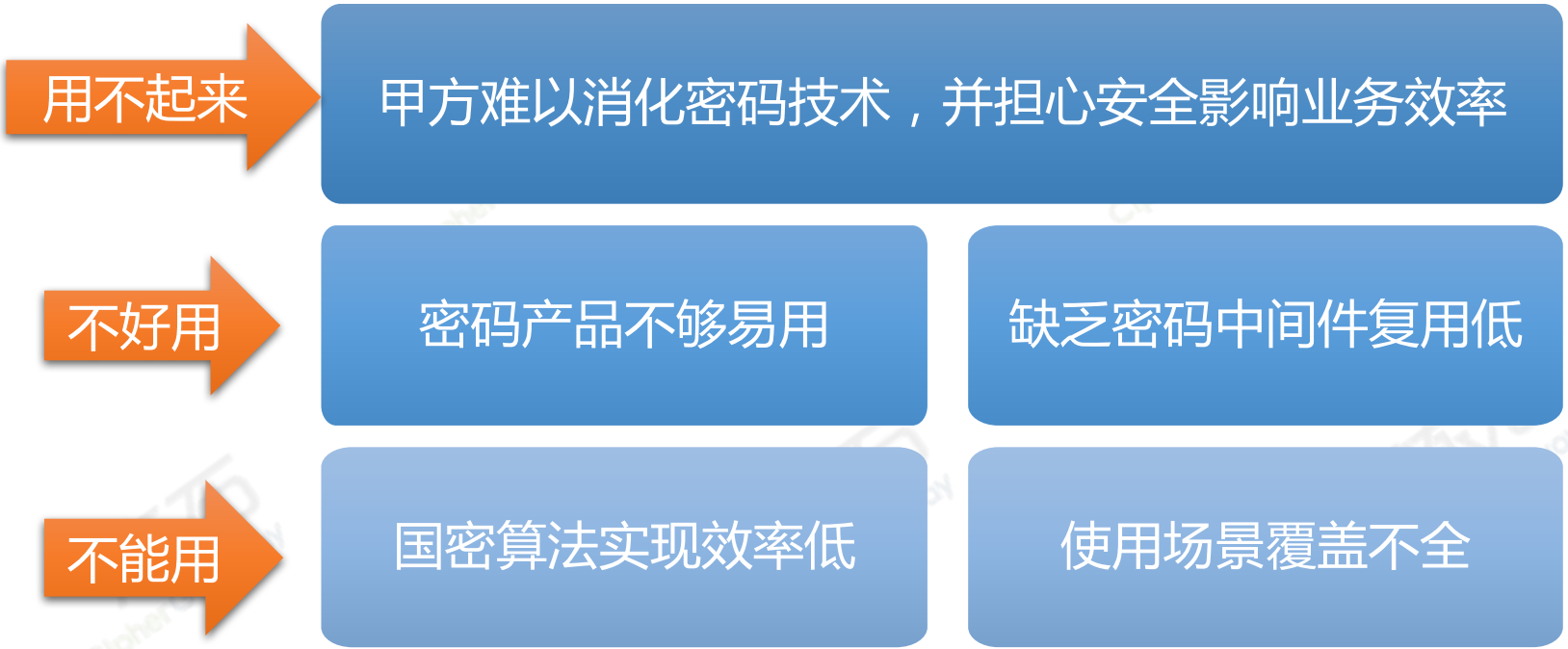
- 密码算法、密码产品、密码应用三者明显脱节
- 有丰富硬件密码产品，但应用普遍缺乏数据安全

* 完整报告《从美国FIPS产品体系浅窥我国密码发展趋势》-V1.0，请联系炼石获取

我国密码产业亟待应用侧补齐和创新



高质量密码供给的三个难题



供给高质量密码，支撑36号文政策落地

密码用起来

行业甲方

结合密码应用模式，在应用新建或改造时，内建密码能力；
将密码及安全适配进业务流程，让数据流转与安全防护兼得；

密码好用

消除使用门槛

提供甲方易用的数据安全产品，
有效防护数据资产、数据共享

降低集成难度

对密码接口进行业务级封装，提炼
中间件，消除集成门槛，降低成本

密码能用

性能卓越

SM系列算法实现性能优化，
可等效替换掉国外算法

场景覆盖完整

覆盖服务器、云端、桌面端、
移动端、物联网端等多种场景

如果密码应用仅止步于“密码四性”和“套餐式采购”……

问：密码能带来什么安全价值？

答： 密码提供保密性、完整性、真实性、不可抵赖性

答： 密码可以保护身份安全、数据安全、业务完整性等

问：我该怎么使用密码技术？

答： 上一套CA、USBKey认证、VPN、密码机的套餐

答： 对重要数据加密就安全了

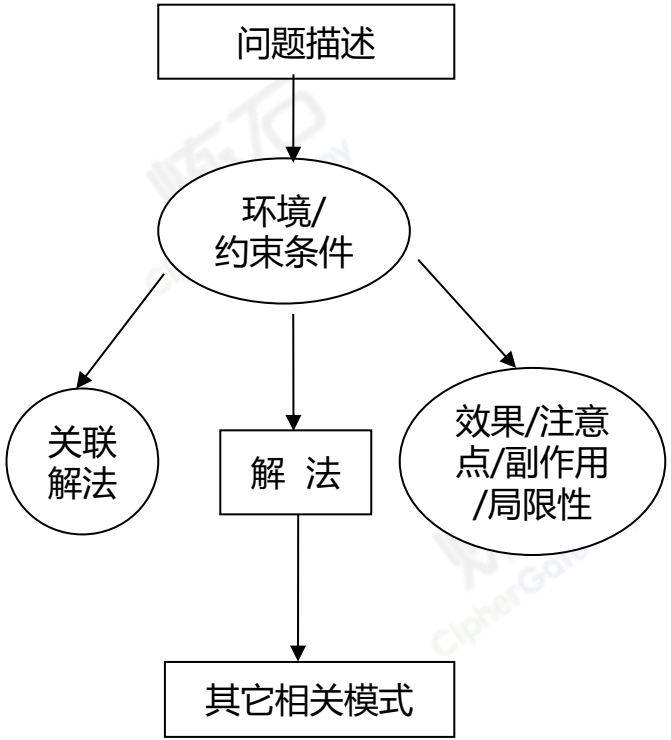
请回答密码使用中的这些问题：

- 对数据不同生命周期阶段，加密防护区别是什么？
- 应用、中间件、基础设施等不同颗粒度对加密需求有何区别？
- 如何用密码技术防护来自业务人员的内部威胁？
- 密码技术如何支撑安全滑动标尺的基础结构安全、纵深防御、积极防御等阶段？
- 结构化和非结构数据等不同类型，防护区别是什么？
- 密码机有多少种类型？使用区别是什么？
- 如何把密码和访问控制、审计等技术有机结合？
- 云计算等新场景下的密码防护手段有哪些？
- ……

2 密码应用模式对密码使用环节创新

密码应用模式可帮用户准确匹配场景

- 密码应用模式是解决特定安全问题的密码方案
  - 模式定义：每个模式都描述了一个在现实环境不断出现的问题，描述该问题的解决方案核心。通过这种方式，可以无数次地使用已有解决方案，无需重复工作。《设计模式：可复用面向对象软件的基础》描述了23种经典面向对象设计模式
  - **密码应用模式定义：提炼出可复用的密码应用设计，提供问题域及解法有关的密码算法、协议清单、安全性说明等，复用密码应用解决方案**，并为甲方、软件集成商、密码厂商、密评机构、监管机构等提供一套标准术语
- 密码应用模式的要素
  - 威胁模型
    - 威胁分析；环境/约束条件；模式威胁示例
  - 模式表述
    - 解法；关联解法；效果/注意点/副作用/局限性
    - 参考案例



炼石提炼22种密码应用模式，推进密码应用创新

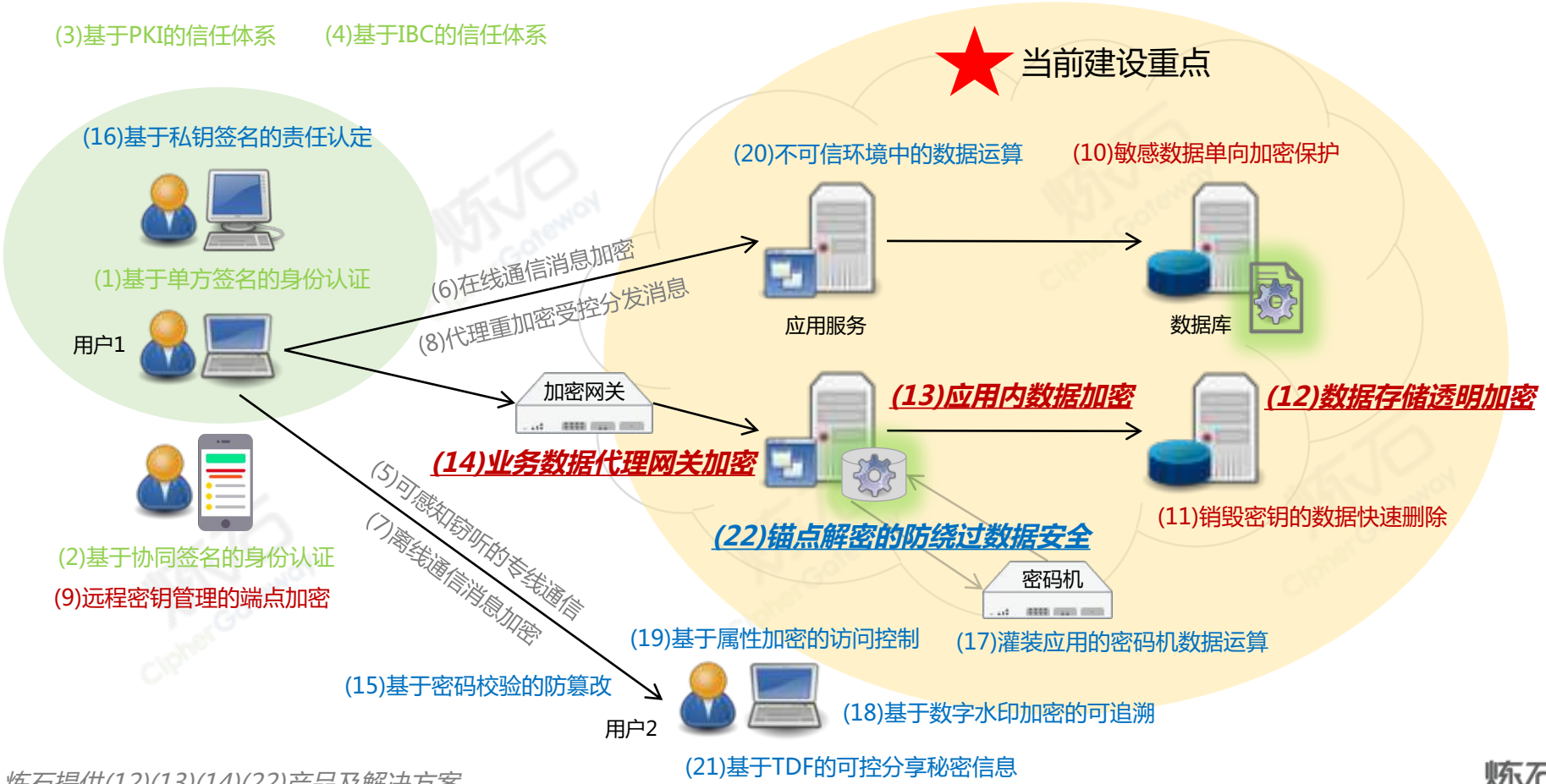
* 数据存储和使用安全是当前建设重心

	身份认证及信任体系 (基础设施)	数据传输 (通信安全)	数据存储 ★ (数据资产安全)	数据使用 ★ (数据共享与安全兼得)
基础型	(1)基于单方签名的身份认证 (2)基于协同签名的身份认证	(5)可感知窃听的专线通信	(9)远程密钥管理的端点加密 (10)敏感数据单向加密保护 (11)销毁密钥的数据快速删除	(15)基于密码校验的防篡改 (16)基于私钥签名的责任认定 (17)灌装应用的密码机数据运算 (18)基于数字水印加密的可追溯 (19)基于属性加密的访问控制
综合型	(3)基于PKI的信任体系 (4)基于IBC的信任体系	(6)在线通信消息加密 (7)离线通信消息加密 (8)代理重加密受控分发消息	***(12)数据存储透明加密*** ***(13)应用内数据加密*** ***(14)业务数据代理网关加密***	(20)不可信环境中的数据运算 (21)基于TDF的可控分享秘密信息 ***(22)锚点解密的防绕过数据安全***

* 基本型采用一种密码算法或安全机制；综合型采用了多种密码算法或安全机制。

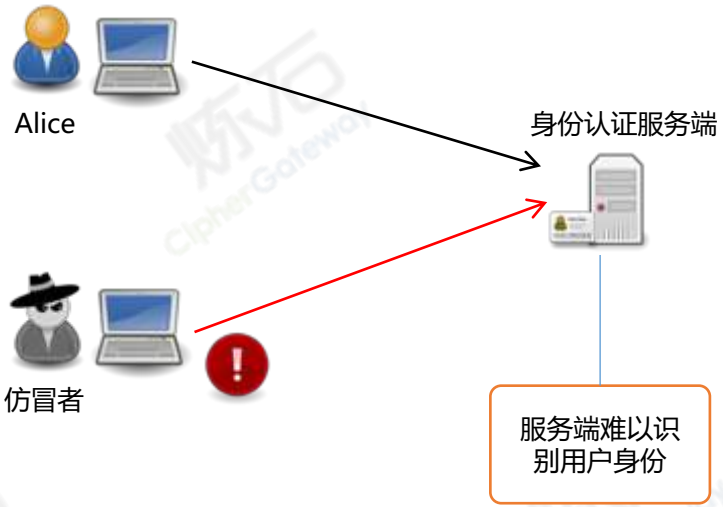
*** 炼石提供(12)(13)(14)(22)产品及解决方案*

当前密码建设重心在于数据存储和使用的保护



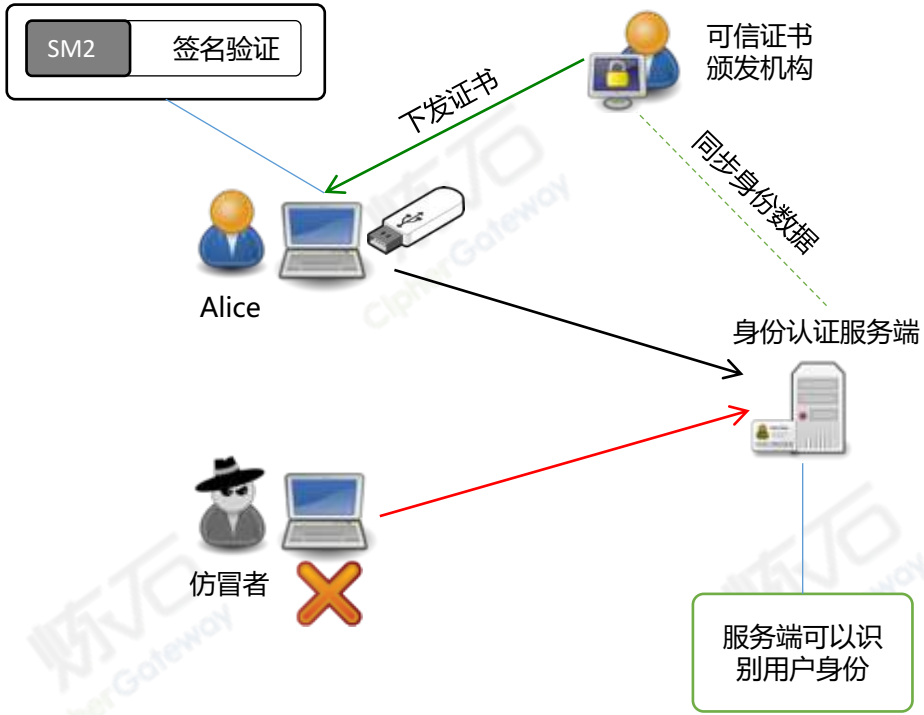
*** 炼石提供(12)(13)(14)(22)产品及解决方案*

模式1-基于单方签名的身份认证：威胁分析



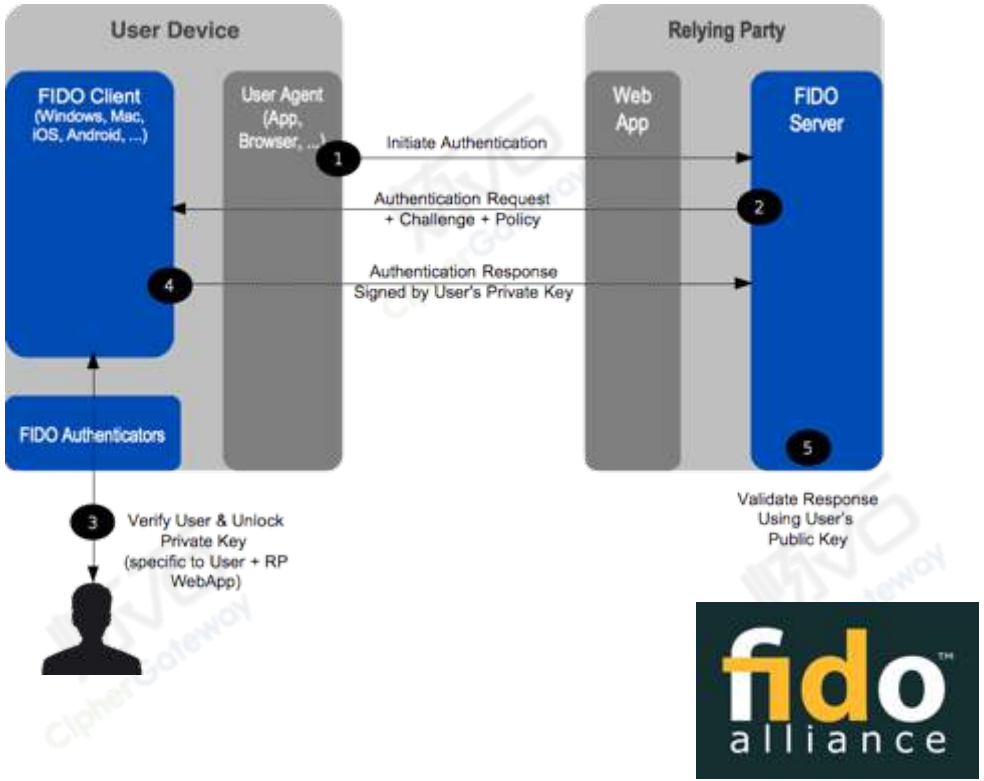
- 威胁分析
  - 【真实性】攻击者可以伪装成用户，向服务端发起请求
- 环境/约束条件
  - 用户存在身份凭证丢失风险，所以要支持吊销
- 模式威胁示例
  - 口令安全性弱，易被仿冒

模式1-基于单方签名的身份认证：防护模型



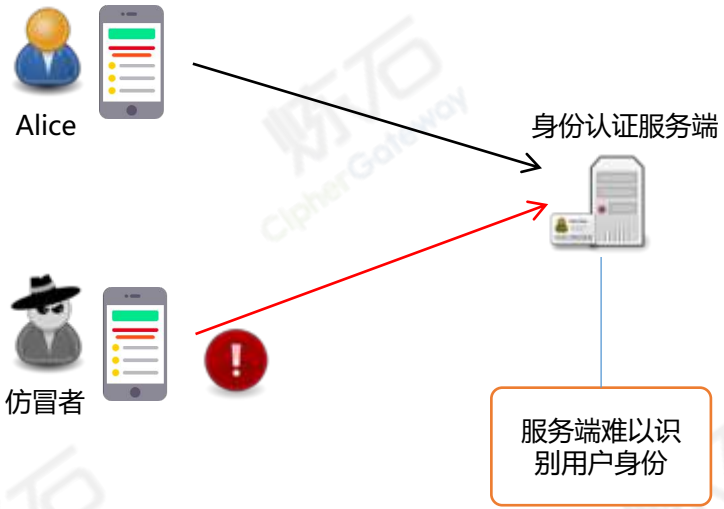
- 解法
  - 基于PKI的身份认证
- 关联解法
  - 用户口令认证
- 效果/注意点/副作用/局限性
  - 用户首次获得证书，需要一个安全通道
- 参考案例
  - 基于密码学的身份认证
  - 网银U盾认证

模式1案例-基于密码技术的的身份认证FIDO



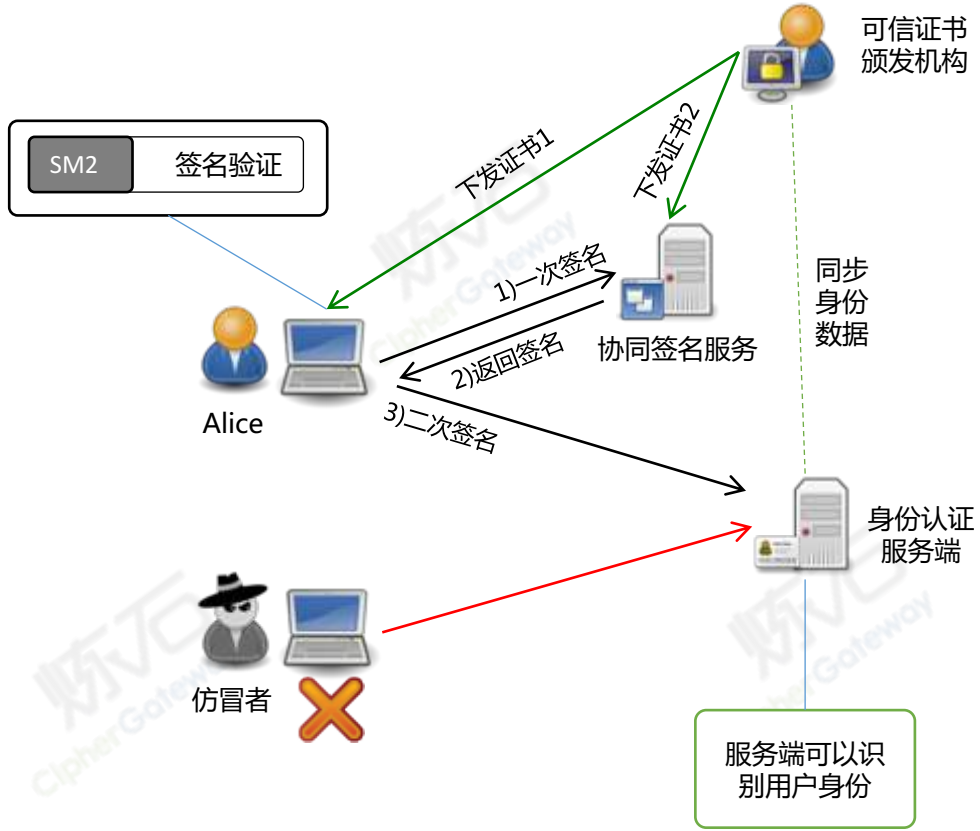
- FIDO（Fast IDentity Online）联盟是成立于2012年7月的行业协会。其宗旨是为解决强制认证设备的交互性和用户面临大量复杂的用户名和密码。
- 2012年7月成立的FIDO联盟，在2014年12月推出了其1.0版本的技术规范，包括致力于“无密码体验”（生物特征）的UAF标准，和“双因子体验”（口令和特定设备）的U2F标准。
- FIDO还可以解决口令或短信验证码等传统移动端认证方式风险过于集中、输入不方便等问题。

模式2-基于协同签名的身份认证-威胁分析



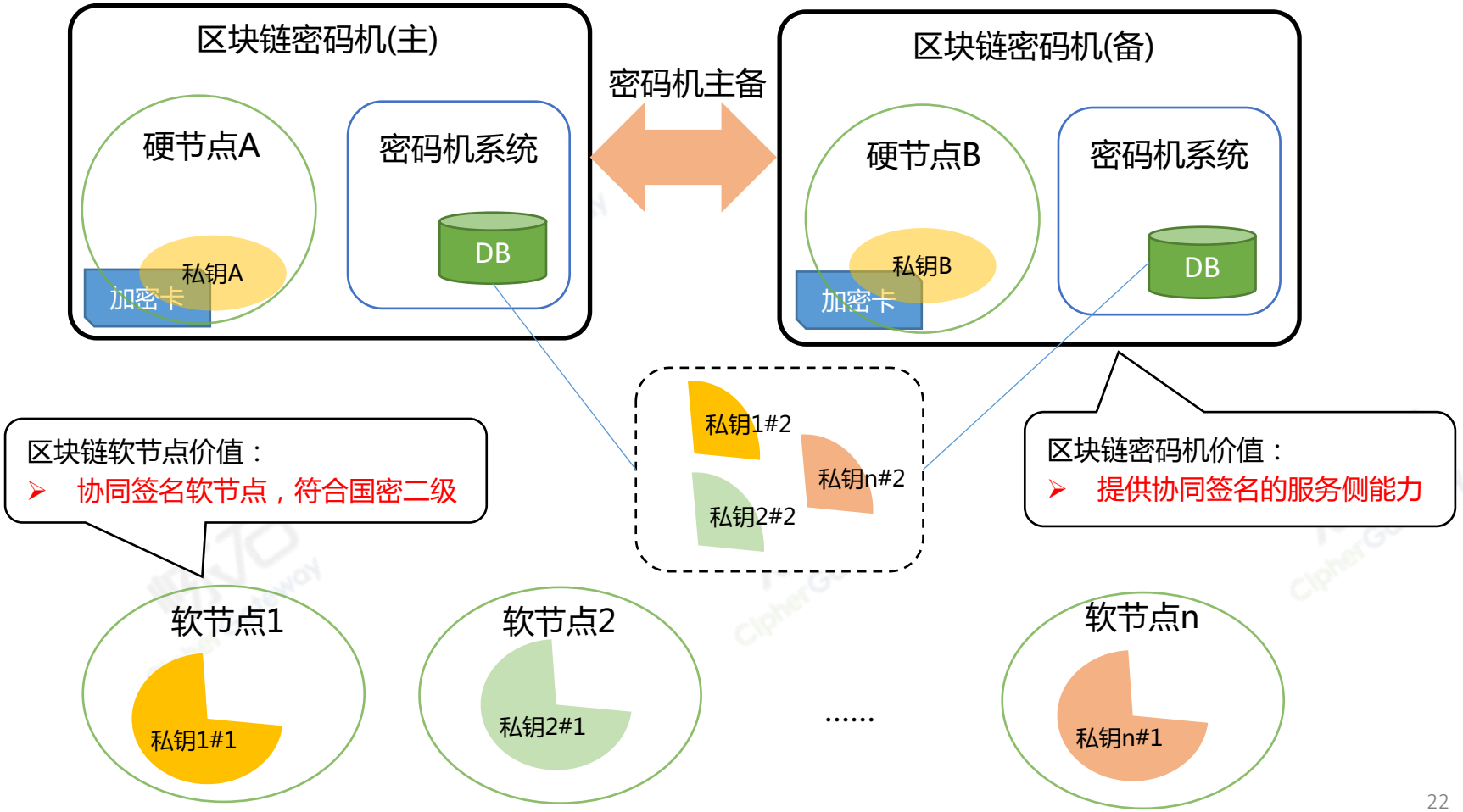
- 威胁分析
  - 【真实性】攻击者可以伪装成用户，向服务端发起请求
- 环境/约束条件
  - 对移动端等环境，很难支持USB Key，只能用软证书
  - 用户存在较高身份凭证丢失风险，但可结合其他身份认证手段
- 模式威胁示例
  - 手机被木马提权，窃取软证书
  - 口令安全性弱，易被仿冒

模式2-基于协同签名的身份认证-防护模型

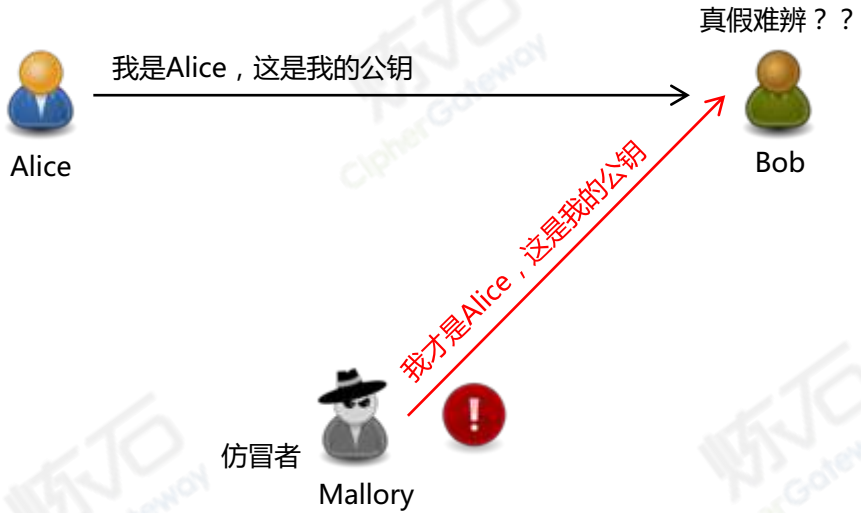


- 解法
  - 基于PKI的身份认证
- 关联解法
  - 用户口令认证
- 效果/注意点/副作用/局限性
  - 用户首次获得证书，需要一个安全通道
- 参考案例
  - 手机网银的协同软认证
  - 虚拟机环境的协同软认证

模式2案例-基于协同签名的国密区块链软节点

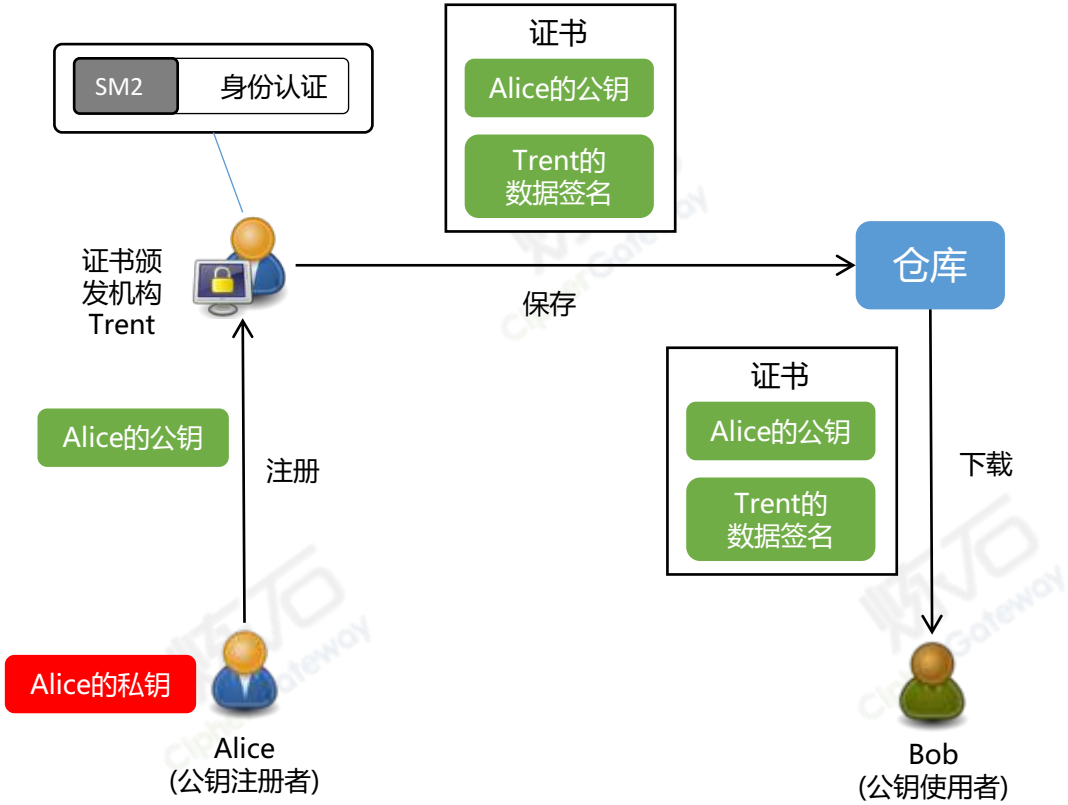


模式3-基于PKI的信任体系-威胁分析



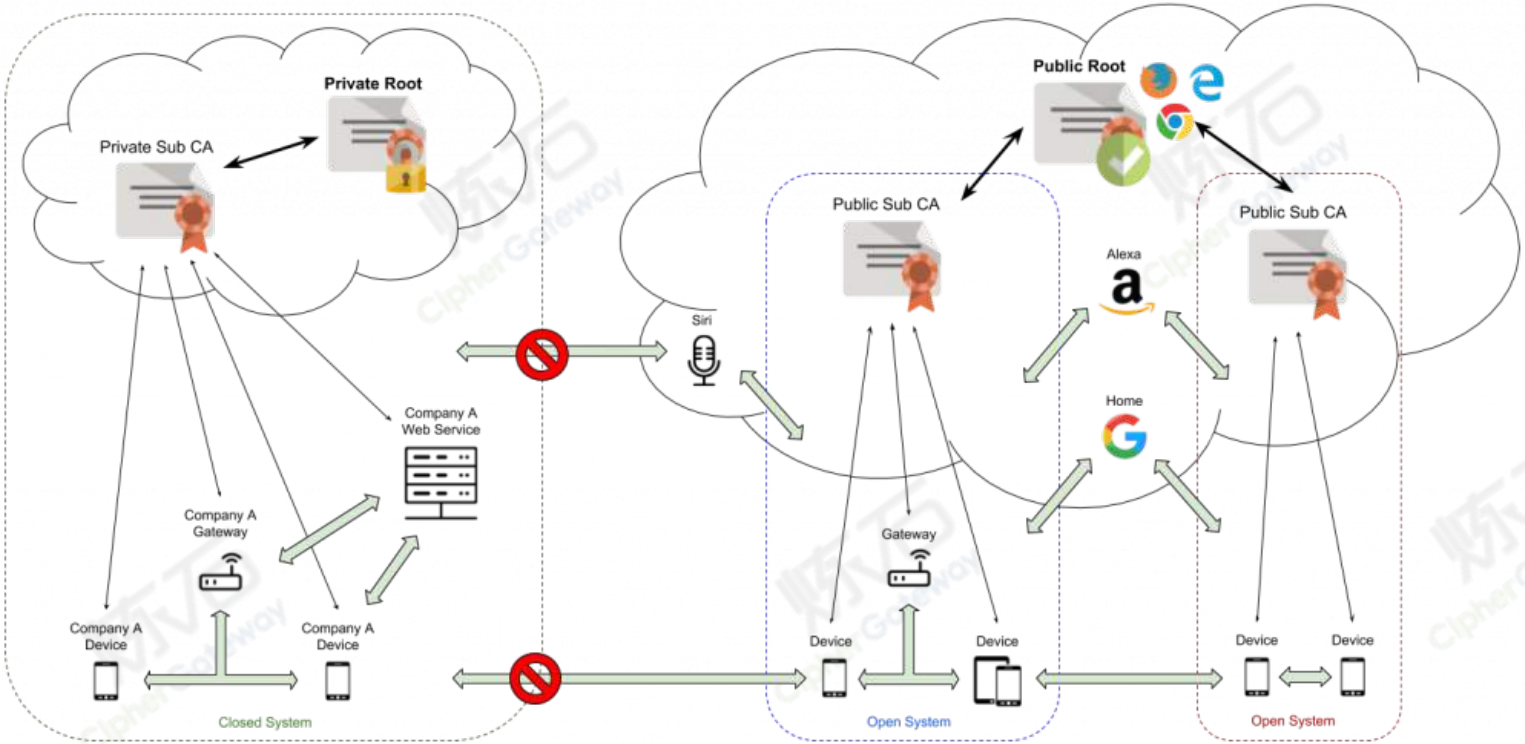
- 威胁分析
  - 网络用户之间无法识别对方身份，容易被攻击者仿冒
- 环境/约束条件
  - 线下预先交换公钥（或共享密钥）的方式，有很大局限性
  - 用户可以预信任一个权威机构
- 模式威胁示例
  - 在缺乏权威证书颁发机构的情况下，容易被攻击者仿冒

模式3-基于PKI的信任体系-防护模型

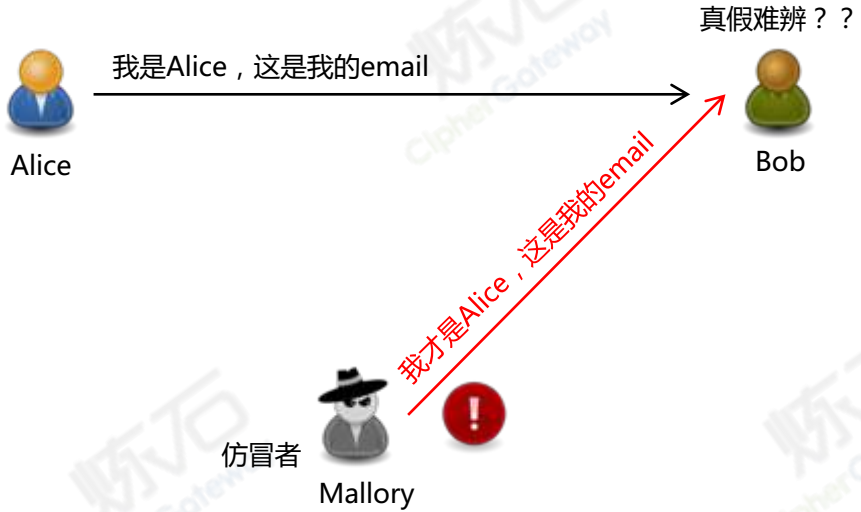


- 解法
  - 公钥基础设施
- 关联解法
  - 线下交换密钥
- 效果/注意点/副作用/局限性
  - Bob需要预先信任Trent
  - Alice私钥可以只有自己拥有，但Alice公钥需要Trent验证Alice身份后颁发
- 参考案例
  - 公共PKI
  - 企业自建PKI

模式3案例-自建CA和公共CA

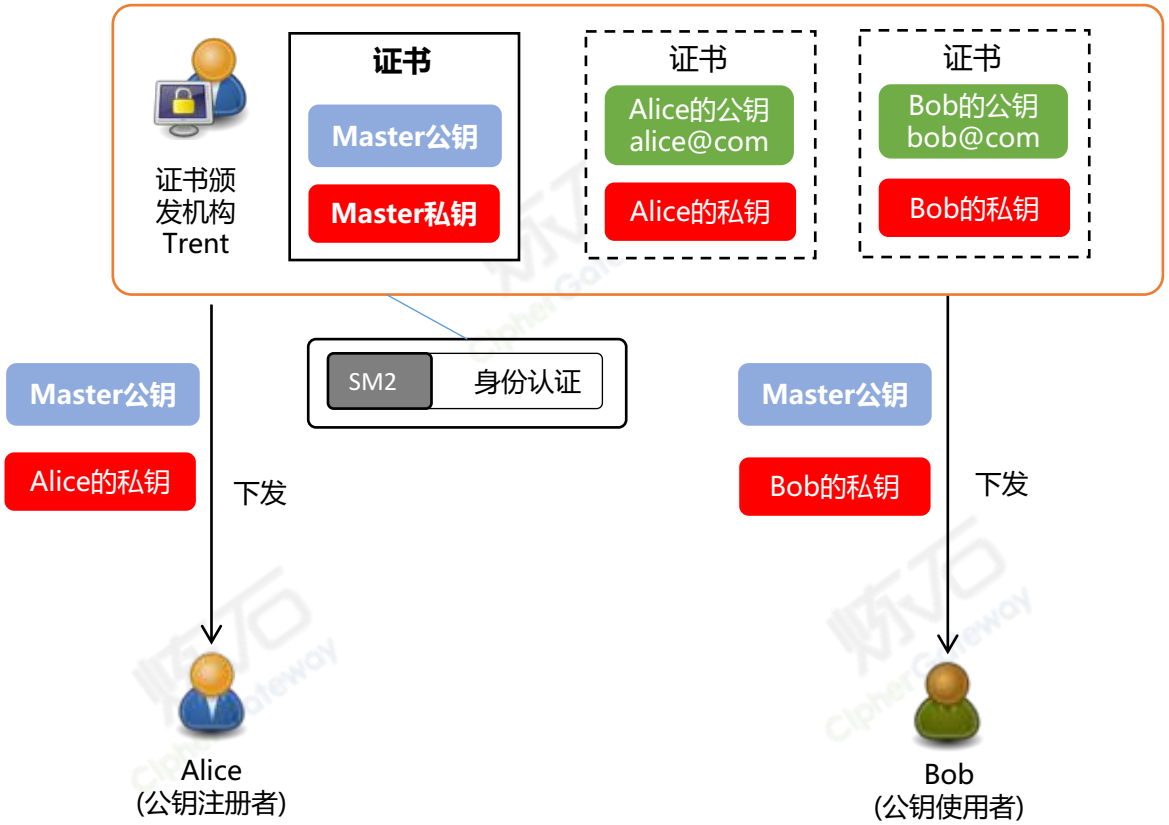


模式4-基于IBC的信任体系-威胁分析



- 威胁分析
  - 网络用户之间无法识别对方身份，容易被攻击者仿冒
- 环境/约束条件
  - 线下预先交换公钥（或共享密钥）的方式，有很大局限性
  - 用户可以绝对信任一个权威机构
- 模式威胁示例
  - 在缺乏权威证书颁发机构的情况下，容易被攻击者仿冒

模式4-基于IBC的信任体系-防护模型



- 解法
  - 公钥基础设施
- 关联解法
  - 线下交换密钥
- 效果/注意点/副作用/局限性
  - Bob需要预先信任Trent
  - Alice私钥可以只有自己拥有，但Alice公钥需要Trent验证Alice身份后颁发
- 参考案例
  - 公共PKI
  - 企业自建PKI

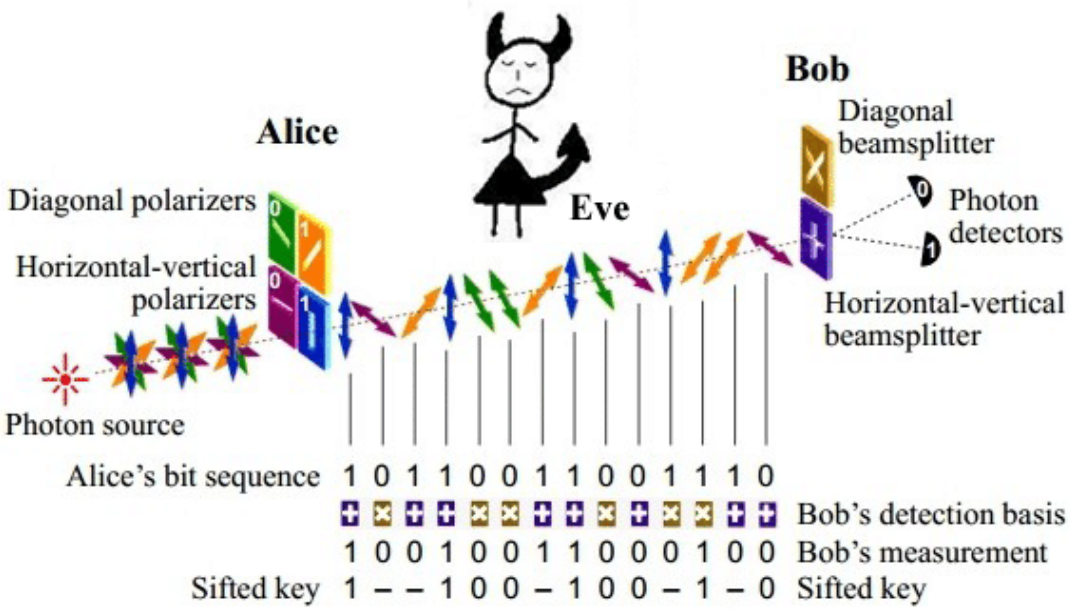
模式5-可感知窃听的专线通信-威胁分析

- 威胁分析
  - 中间人Eve窃听
  - 中间人Mallory篡改
- 环境/约束条件
  - 假如被Eve窃听，Alice和Bob都不知情
- 模式威胁示例
  - 实时通信被劫持

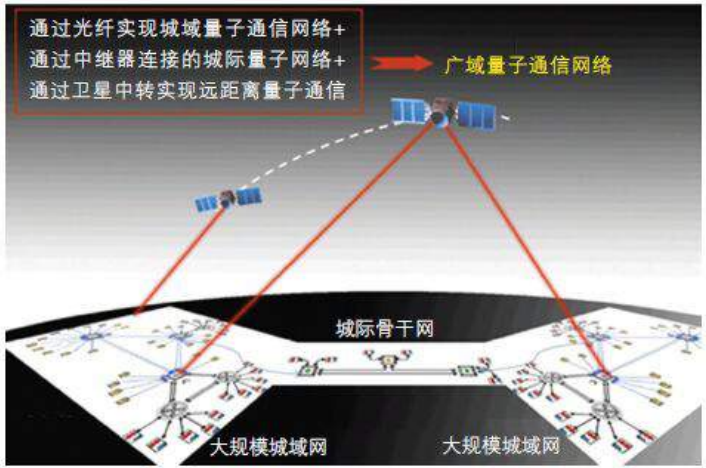
模式5-可感知窃听的专线通信-防护模型

- 解法
  - 基于BB84的量子密钥分发
- 关联解法
  - 物理安全专线，但无法感知窃听
- 效果/注意点/副作用/局限性
  - 缺乏身份认证
  - 带宽很低
  - 工程实现难度极大
- 参考案例
  - 量子密钥分发网络

模式5案例-QKD量子密钥分发

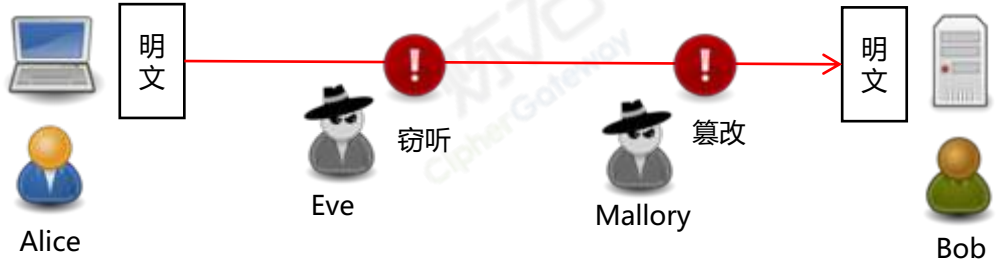


基于BB84协议的量子密钥分发



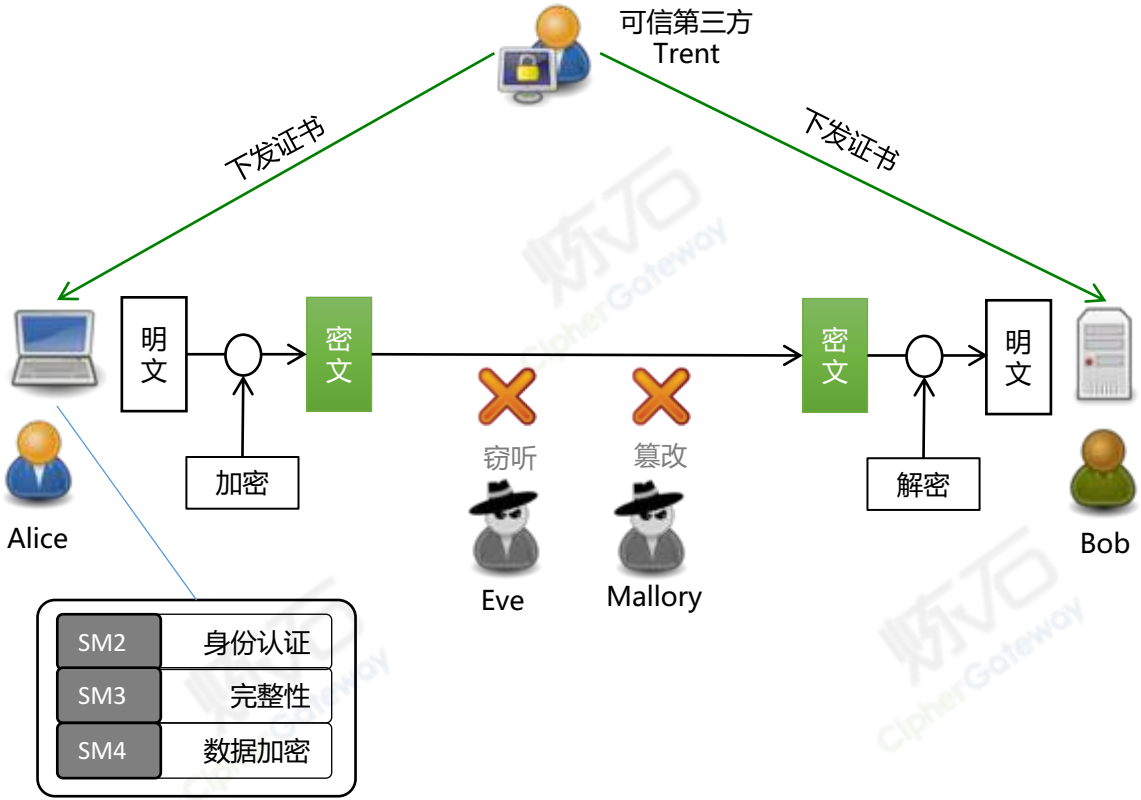
墨子号科学实验卫星

模式6-在线通信消息加密：威胁分析



- 威胁分析
  - 中间人Eve窃听
  - 中间人Mallory篡改
- 环境/约束条件
  - Bob是在线服务提供者
  - 当Alice向Bob发起请求，Bob会实时响应
- 模式威胁示例
  - 实时通信被劫持
  - 用户浏览网站被劫持
  - 服务调用被劫持

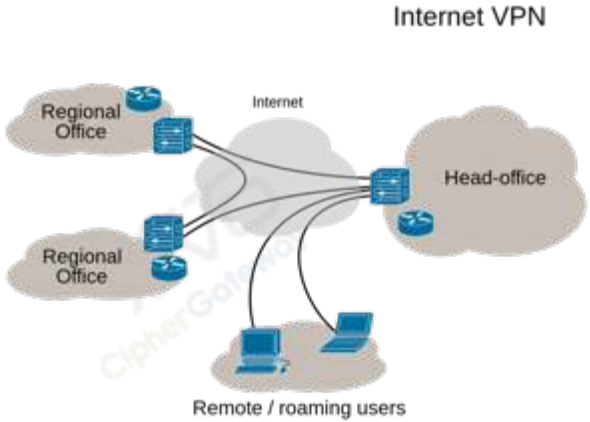
模式6-在线通信消息加密：防护模型



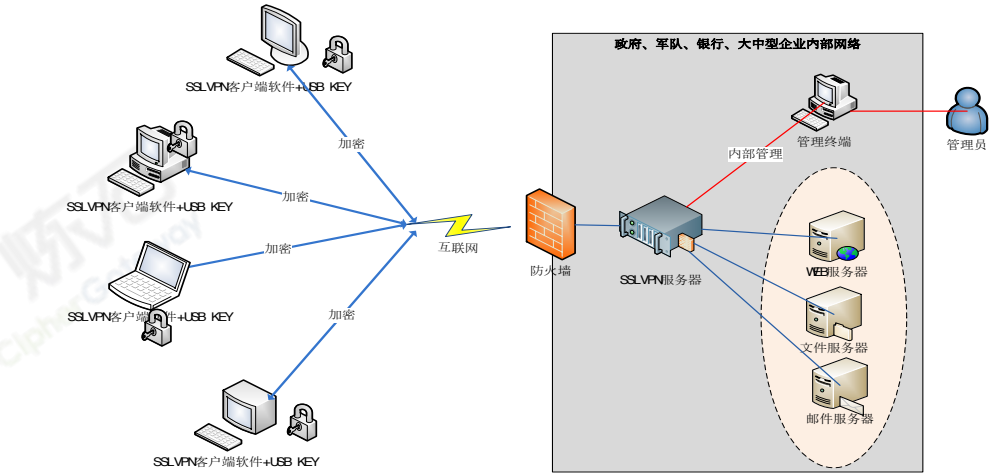
- 解法
  - 标准TLS协议的各种实现
  - TLS扩展
    - HTTPS
    - SMTP/IMAP/POP3 over TLS
    - SSL VPN
  - 验证方式
    - 单向SSL
    - 双向SSL
  - 推荐软件选择：MesaLink/OpenSSL
- 关联解法
  - SSH方案，比如OpenSSH
  - IPSec VPN
- 效果/注意点/副作用/局限性
  - TLS会增加约5-10%的服务端资源消耗
- 参考案例
  - VPN保护商业秘密信息在互联网传输
  - HTTPS保护Web应用中数据传输安全

模式6案例-常见VPN示例

IPSec VPN

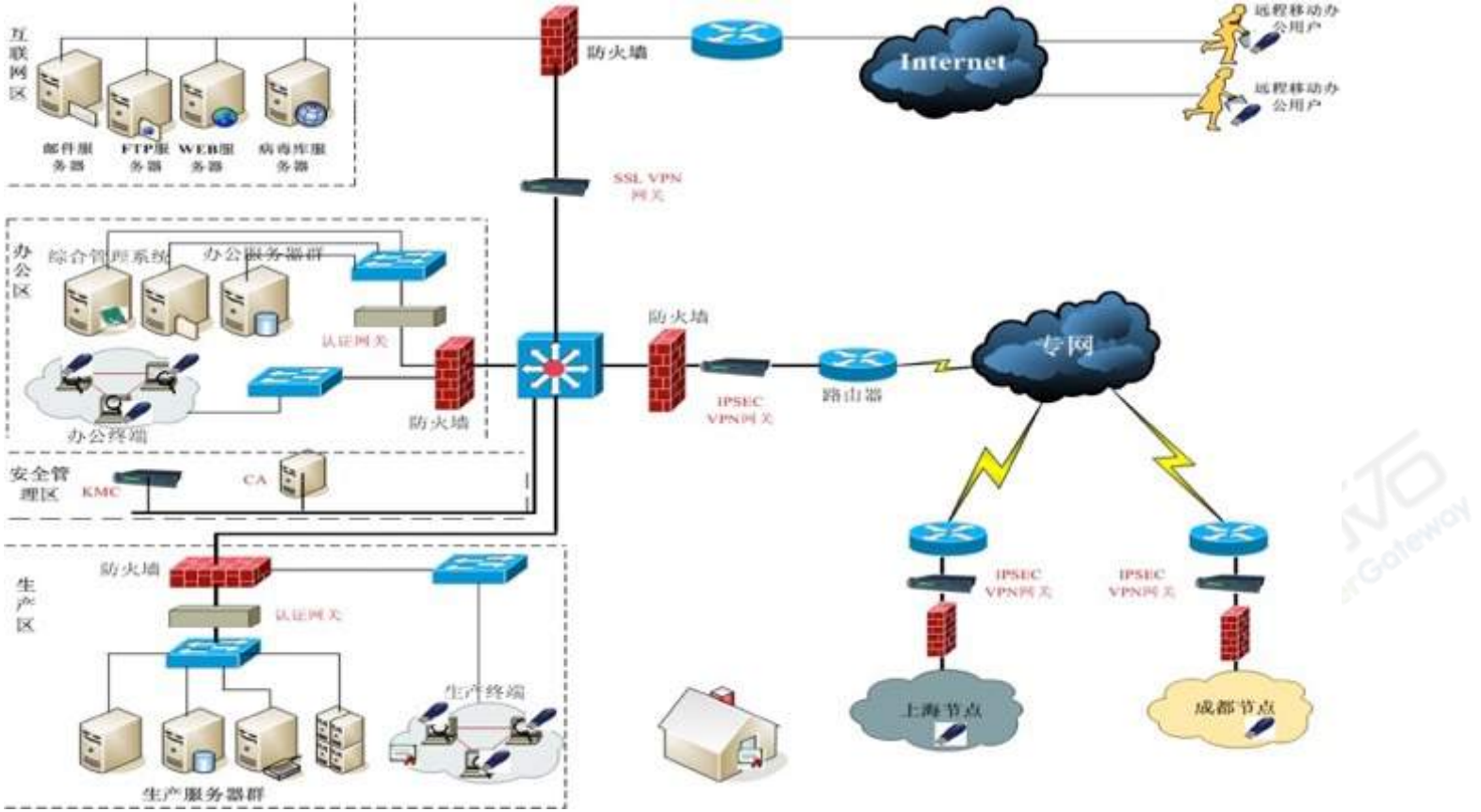


SSL VPN

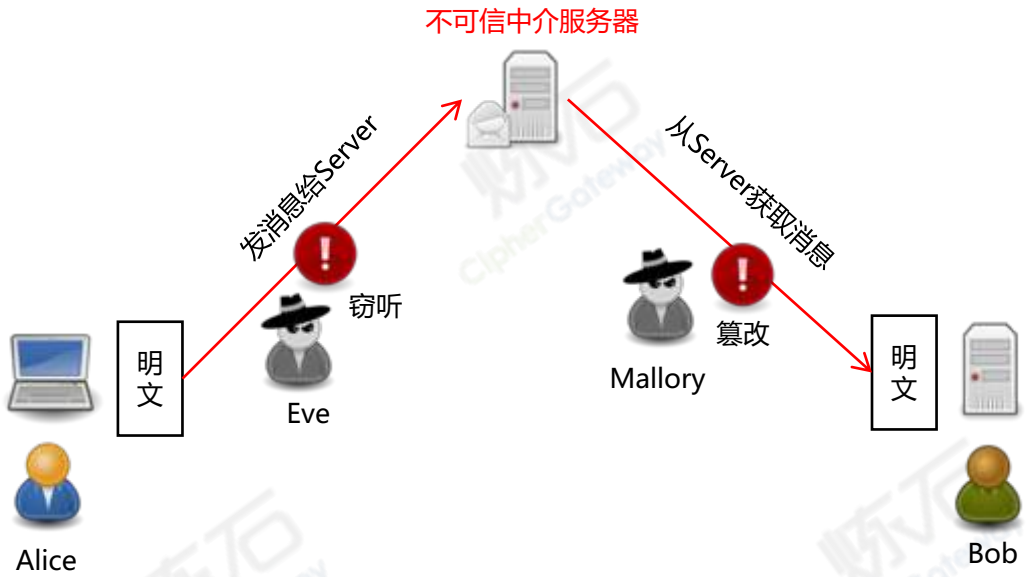


- 当使用互联网服务服务处理商业秘密信息，可采用VPN技术保护
- IPSec VPN是基于IP网络的VPN，适用于总部与分支机构之间
- IPSec VPN是基于SSL/TLS协议的VPN，支持浏览器接入，适用于用户从远程接入

模式6案例-某集团企业通信加密案例（两种VPN）

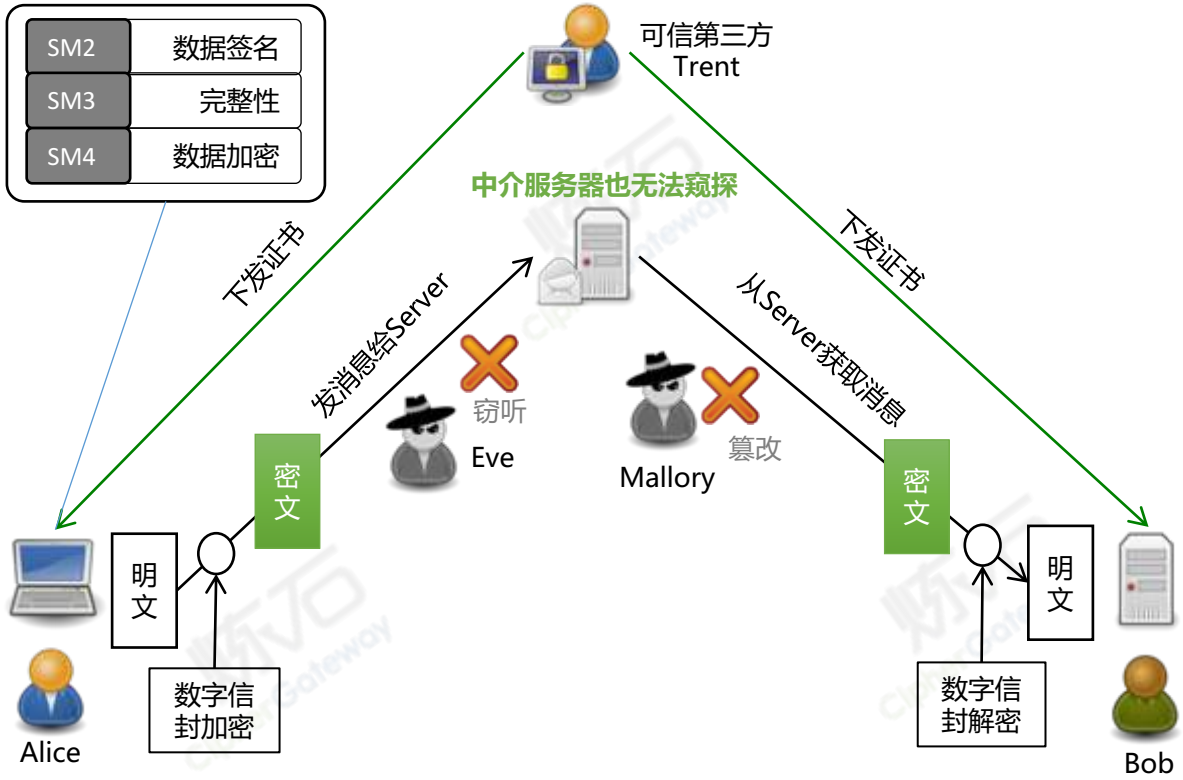


模式7-离线通信消息加密：威胁分析



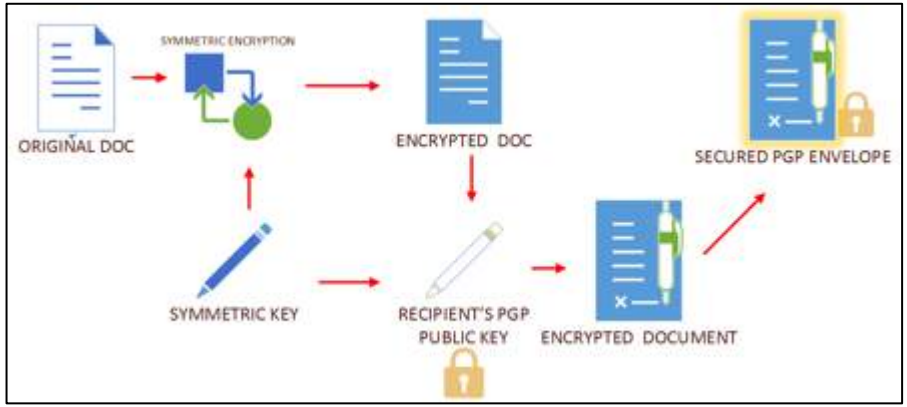
- 威胁分析
  - 中间人Eve窃听
  - 中间人Mallory篡改
- 环境/约束条件
  - 对Alice来讲Bob是离线状态
  - Alice把消息发给服务器，Bob定期从服务器更新消
- 模式威胁示例
  - 发邮件被劫持
  - 发短信被劫持
  - IM聊天被劫持

模式7-离线通信消息加密：防护模型

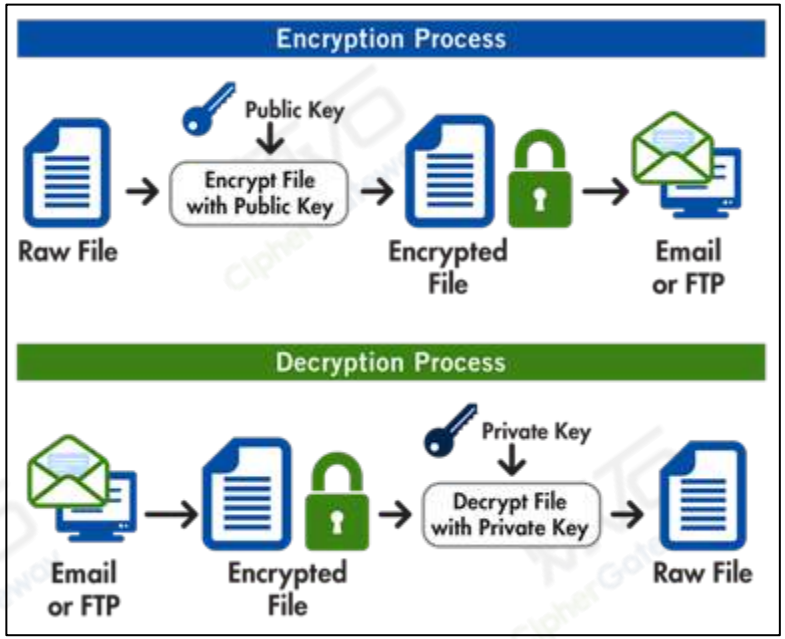


- 解法
  - 基于PKI的数字信封加密
  - 推荐软件：GnuPG
- 关联解法
  - ID-based encryption
    - PKG及证书机制有待完善
    - SM9算法性能远低于SM2
- 效果/注意点/副作用/局限性
  - 通信双方需要对方公钥
- 参考案例
  - 商业秘密通过PGP邮件安全收
  - 防范短信敏感信息泄露或篡改

模式7案例-PGP邮件安全

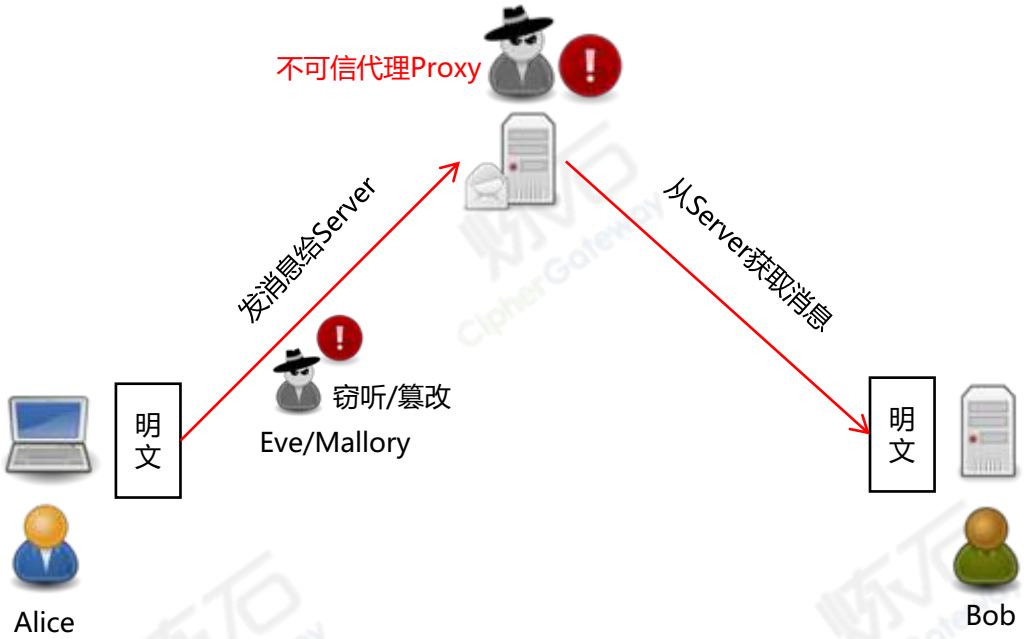


数字信封加密，用到SM2/SM3/SM4等算法



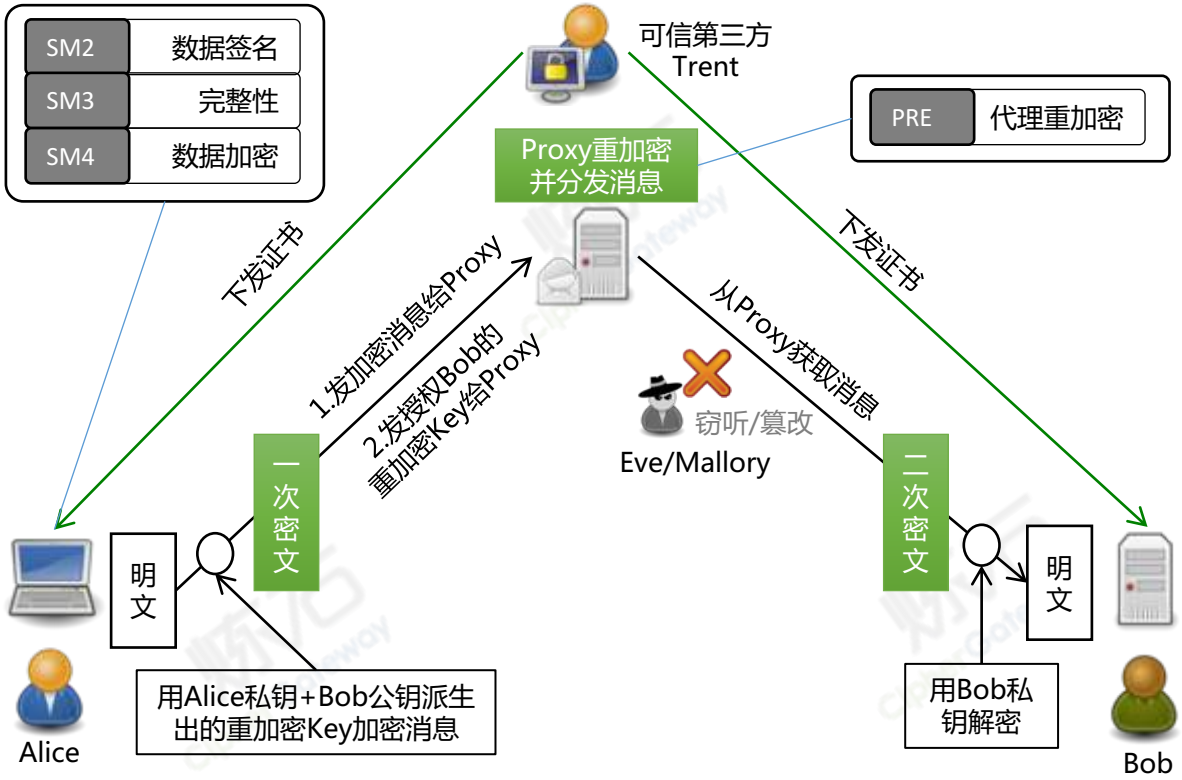
PGP通信流程

模式8-代理重加密受控分发消息：威胁分析



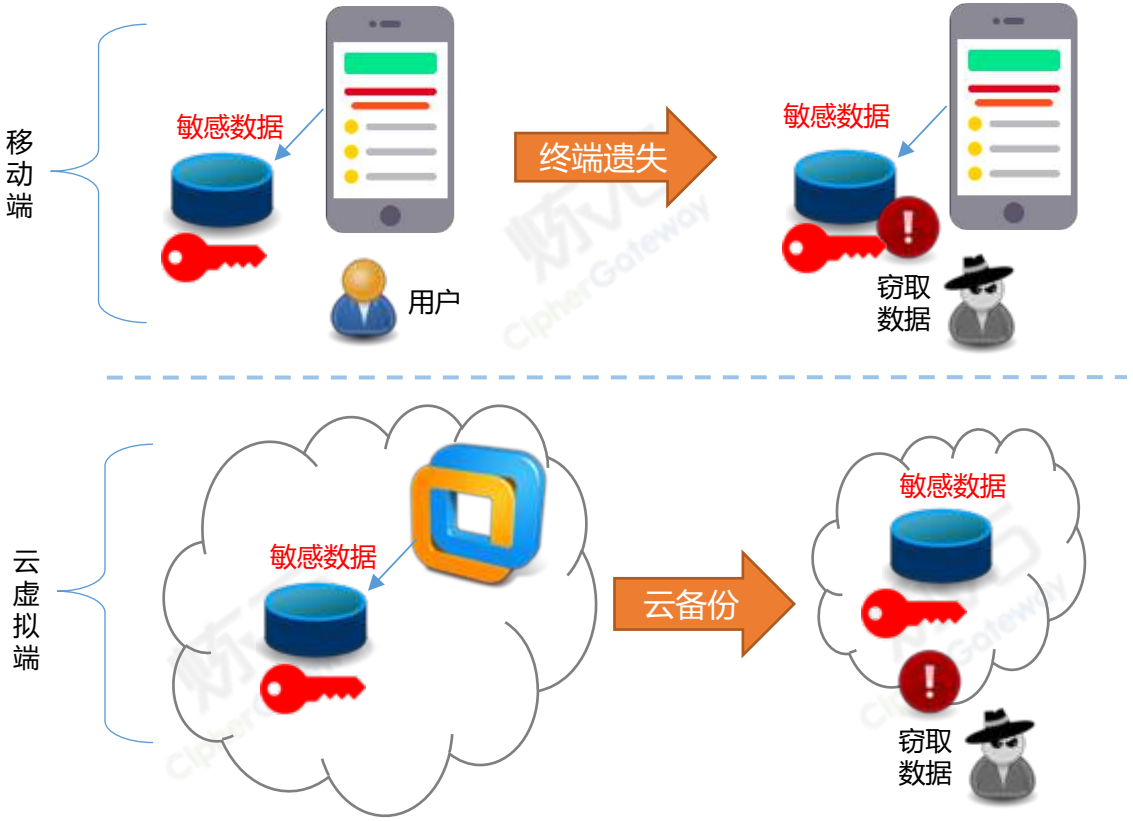
- 威胁分析
  - 代理Proxy窃听和篡改消息
  - 传统中间人窃听和篡改消息
- 环境/约束条件
  - Alice发消息给Proxy委托时，并不确定消息要发给哪些接收者；或Alice无法直接与Bob通信
  - Proxy可以提供二次加密服务
- 模式威胁示例
  - 网盘代理分发共享秘密文件

模式8-代理重加密受控分发消息：防护模型



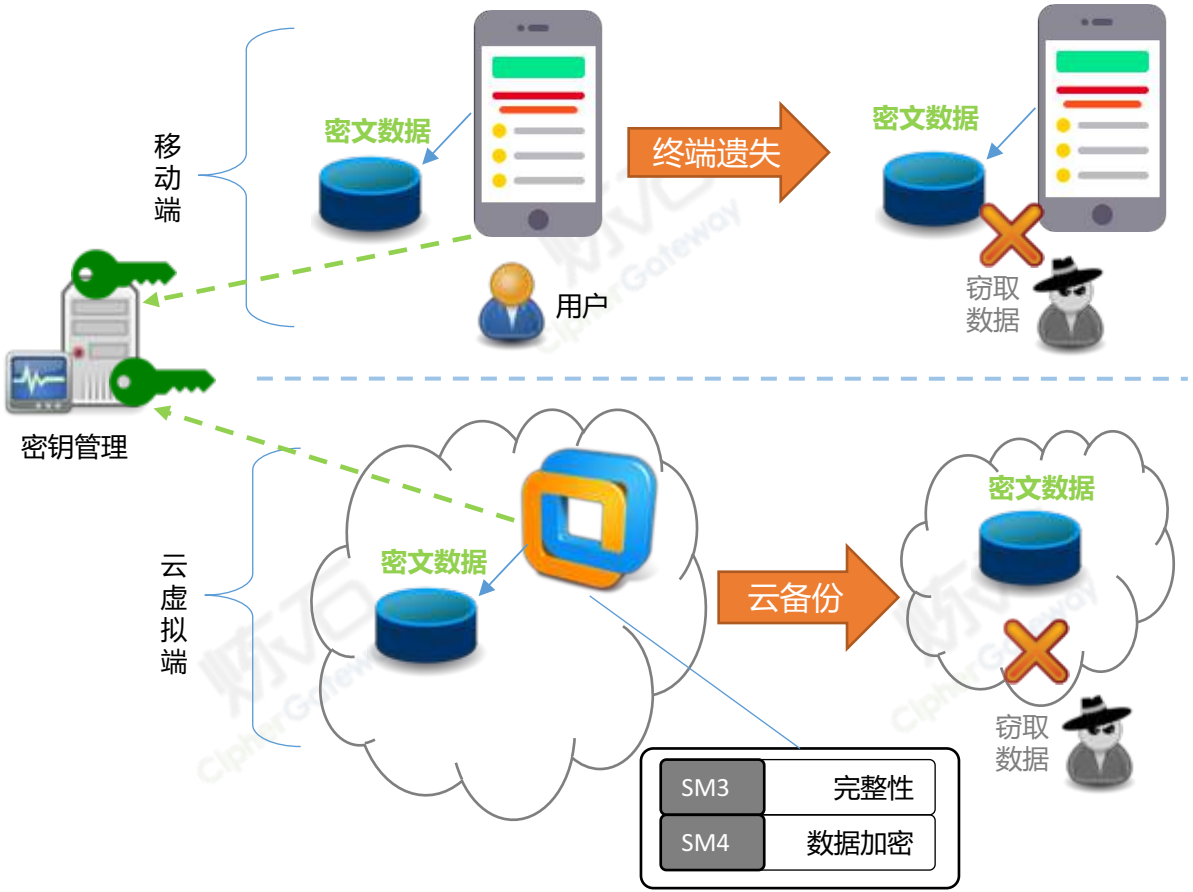
- 解法
  - 基于PRE+PKI的数字信封加密
  - 推荐软件：无
- 关联解法
  - PGP邮件加密
- 效果/注意点/副作用/局限性
  - **Alice解耦了消息加密动作、和授权Bob解密，增加了管控灵活度**
  - 通信双方需要对方公钥
- 参考案例
  - 网盘二次分发机密信息
  - 企业内文件授权分发

模式9-远程密钥管理的端点加密：威胁分析



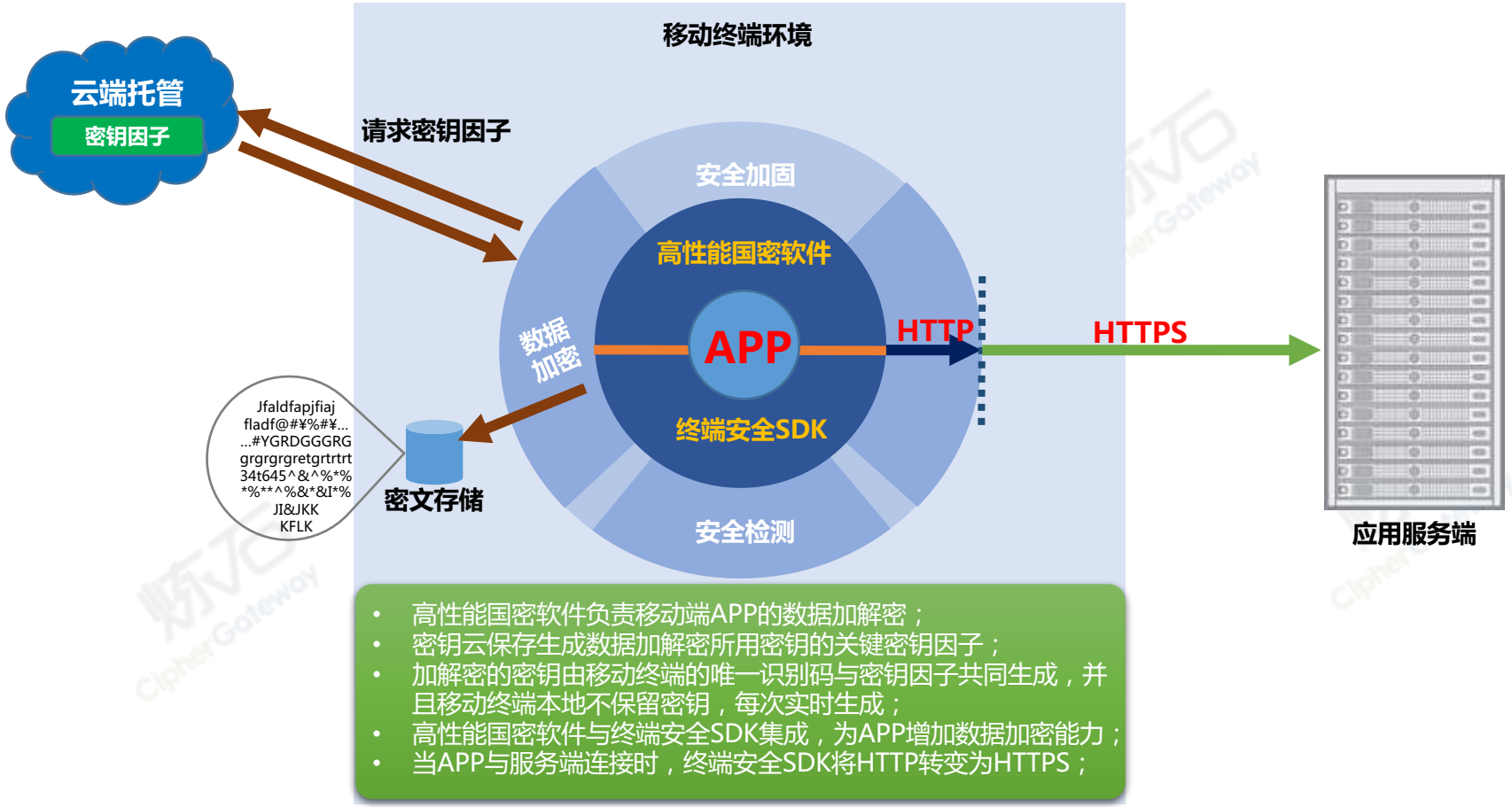
- 威胁分析
  - 终端敏感数据存在攻击者非法访问风险
- 环境/约束条件
  - 终端具有加密能力，但缺失安全的密钥存储机制如HSM
- 模式威胁示例
  - 手机丢失被拔卡窃取数据
  - 云虚拟机数据被泄露

模式9-远程密钥管理的端点加密：防护模型



- 解法
  - 终端完成加密，但密钥保存在远程KMS，KMS提供安全策略
- 关联解法
  - 密钥保存在终端存储，安全威胁较大
- 效果/注意点/副作用/局限性
  - 终端需要联网才能运行
  - 同时终端身份认证也是难点
- 参考案例
  - 移动端存储加密防范数据泄露
  - 云虚拟机加密防范数据泄露

模式9案例-远程密钥管理的移动终端加密

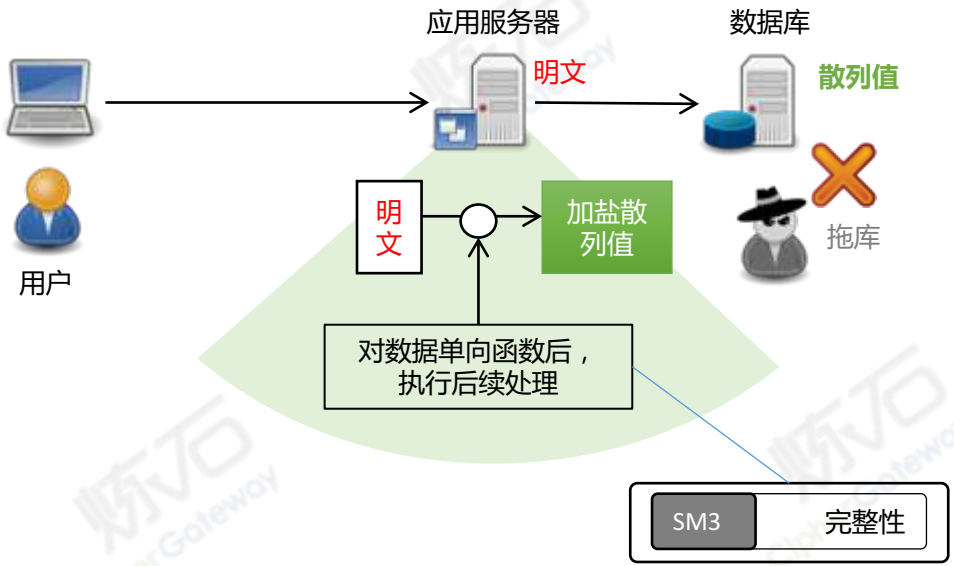


- 高性能国密软件负责移动端APP的数据加解密；
- 密钥云保存生成数据加解密所用密钥的关键密钥因子；
- 加解密的密钥由移动终端的唯一识别码与密钥因子共同生成，并且移动终端本地不保留密钥，每次实时生成；
- 高性能国密软件与终端安全SDK集成，为APP增加数据加密能力；
- 当APP与服务端连接时，终端安全SDK将HTTP转变为HTTPS；

模式10-敏感数据单向加密保护：威胁分析

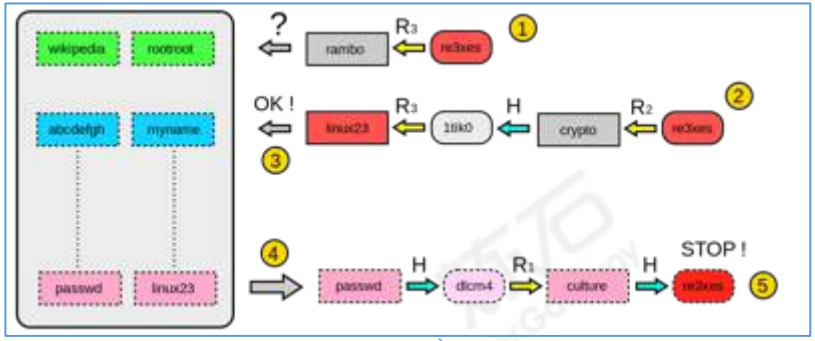
- 威胁分析
  - 敏感数据在传输、使用、存储过程中，都存在泄漏风险
- 环境/约束条件
  - 敏感数据只需判断是否相等
- 模式威胁示例
  - 用户口令传输、使用、存储中的泄露

模式10-敏感数据单向加密保护：防护模型

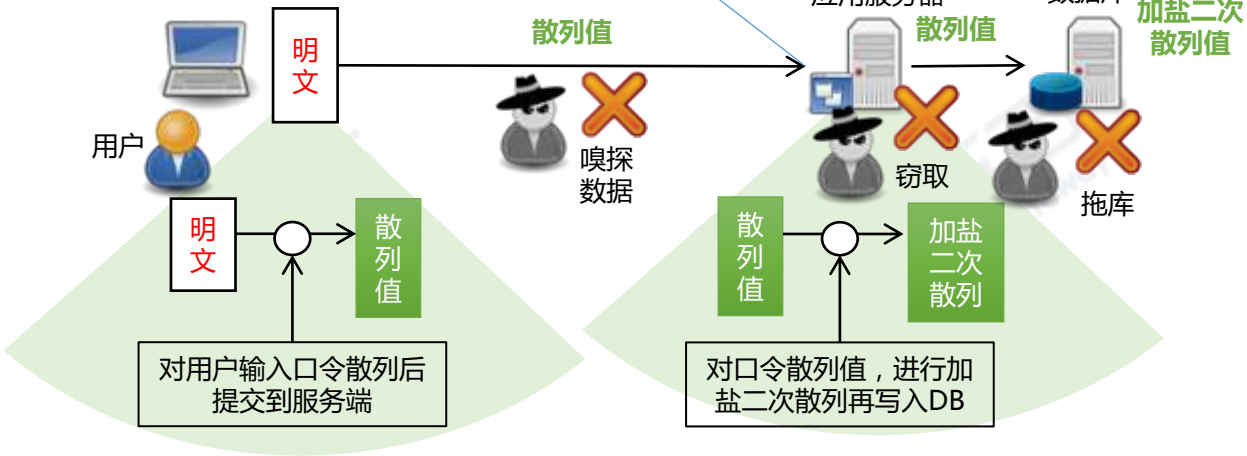


- 解法
  - 敏感数据全生命周期，采用单向加密函数结果值，避免明文暴露
- 关联解法
  - 加密后存储：如果密钥泄露敏感数据能被解密
- 效果/注意点/副作用/局限性
  - 系统只能重置敏感数据，适用于特定场景
- 参考案例
  - 基于散列函数的口令安全防护
  - 无法吊销的生物认证敏感数据处理

模式10案例-基于散列函数的口令防护机制



复杂加盐多次散列
抵抗彩虹表攻击



- 用户端输入口令后，散列后再提交服务端。同时输入口令可采用安全控件加强防护
- 应用服务器收到用户端提交口令散列后，生成复杂盐值并和口令散列进行二次散列处理，保存盐值和二次散列值
- 比较口令时，只比对二次散列值
- 采用HTTPS加强通信安全防护
- 保证了口令全生命周期处理中的安全防护

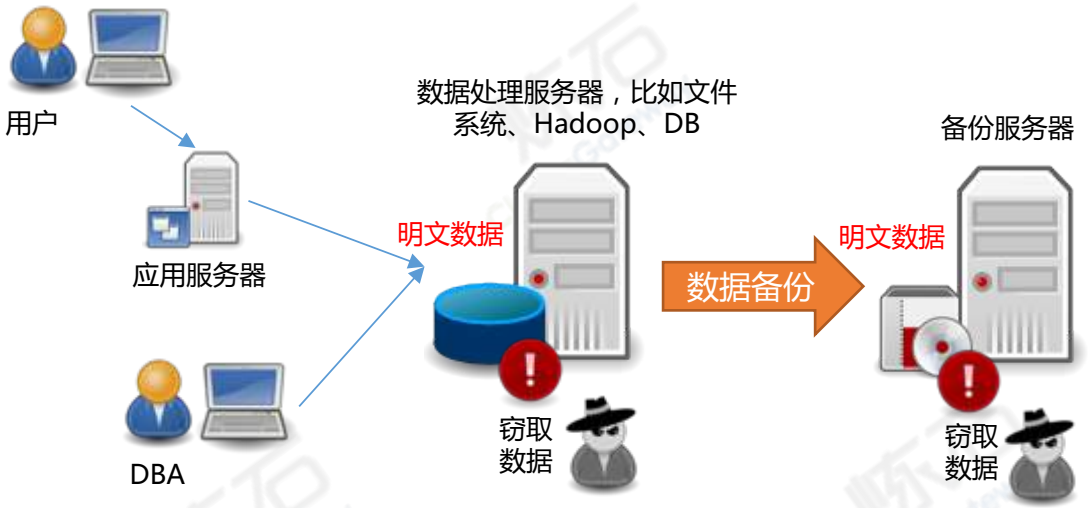
模式11-销毁密钥的数据快速删除：威胁分析

- 威胁分析
  - 有限时间内，无法快速彻底删除数据，落入敌手后被分析还原
- 环境/约束条件
  - 磁盘物理格式化耗时较长
- 模式威胁示例
  - 军事场景磁盘落入敌手

模式11-销毁密钥的数据快速删除：防护模型

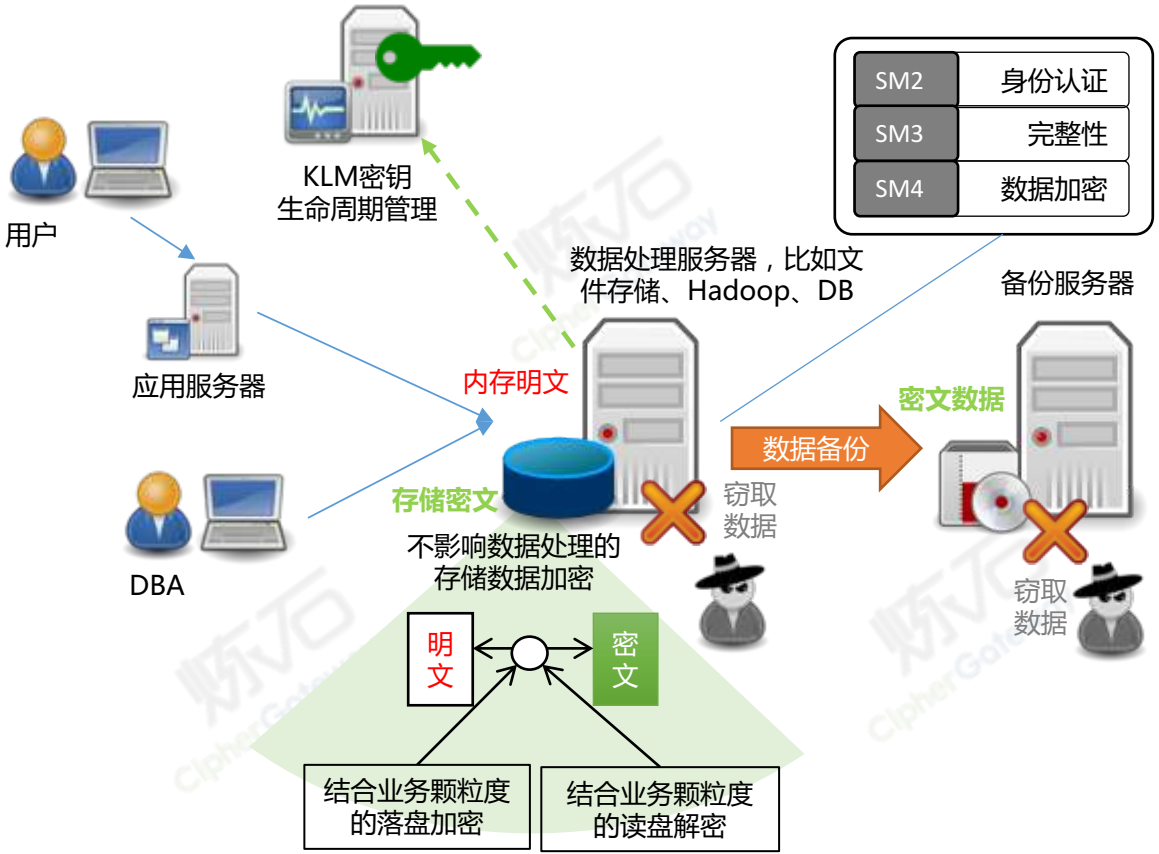
- 解法
  - 销毁逐级密钥的数据快速删除
- 关联解法
  - 磁盘低格，或磁盘物理捣毁
- 效果/注意点/副作用/局限性
  - 兼具 “防拔盘”效果
  - 密钥管理要做好
- 参考案例
  - 特定场景下的磁盘快速删除

模式12-数据存储透明加密：威胁分析



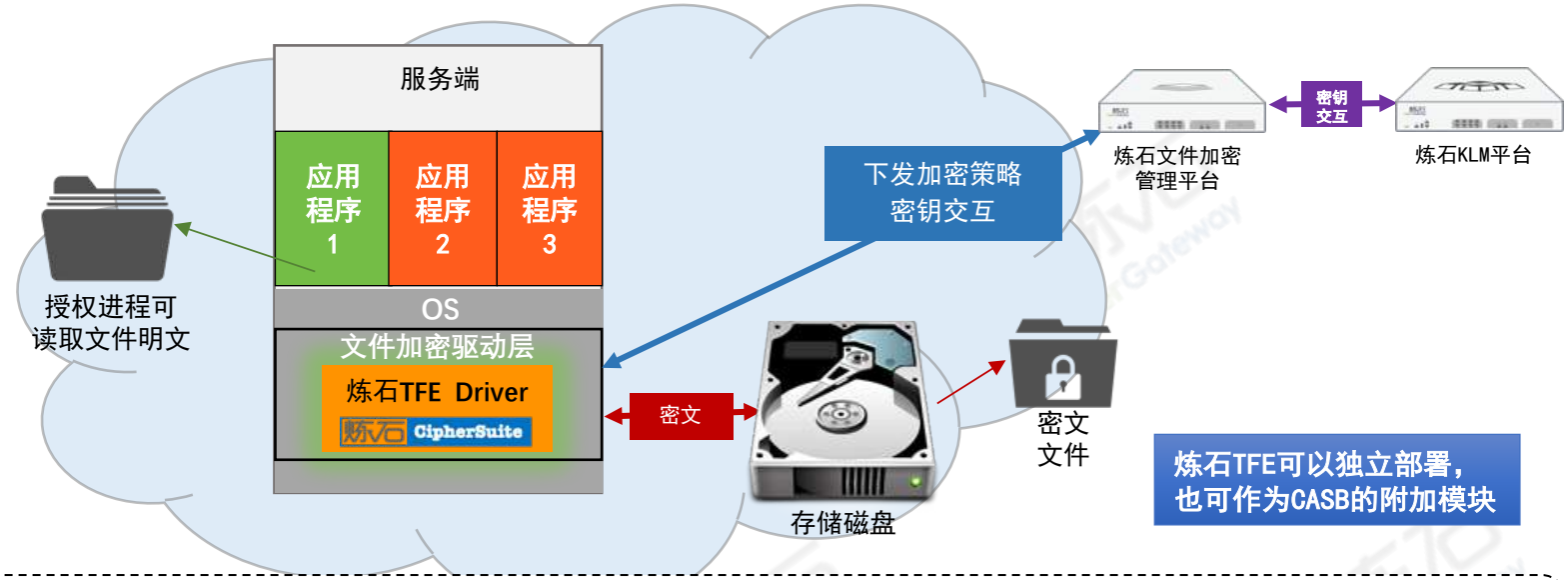
- 威胁分析
  - 攻击者可以从服务端或备份文件窃取敏感数据
- 环境/约束条件
  - 数据计算前需要先解密
- 模式威胁示例
  - 文件存储明文落盘
  - Hadoop数据明文落盘
  - 数据库明文落盘

模式12-数据存储透明加密：防护模型



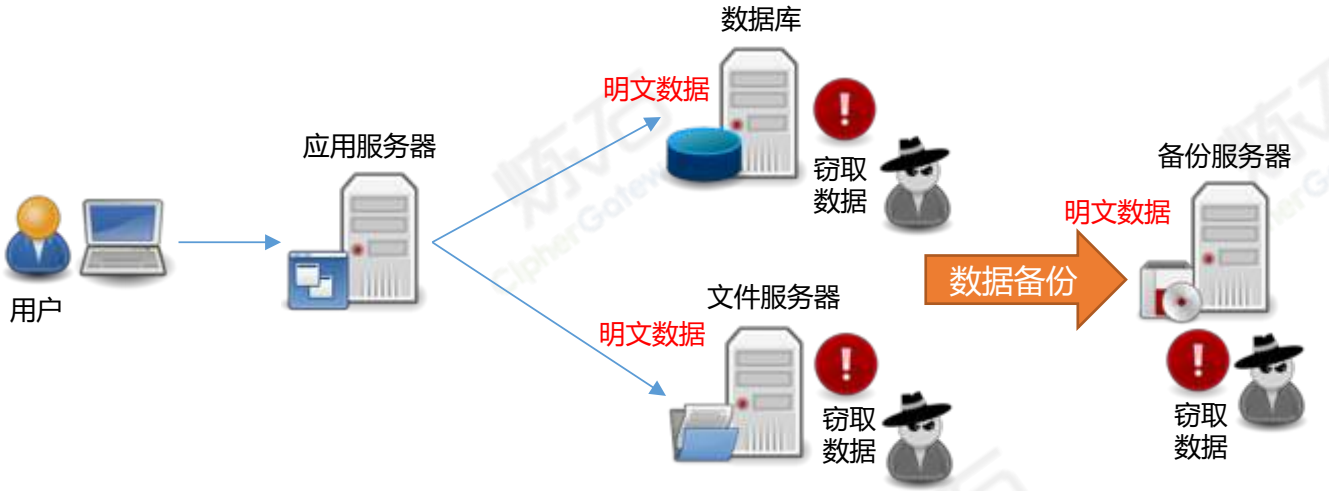
- 解法
  - 结合文件存储、Hadoop或DB，对文件、块文件、表空间等进行加密
- 关联解法
  - 全磁盘加密：粒度粗，只能防拔盘
  - 部署在应用与DB间的数据库加密网关：密文计算难以工业级交付
- 效果/注意点/副作用/局限性
  - 要结合目标文件系统、或数据库品牌版本等
- 参考案例
  - TFE透明文件加密防商业文档泄露
  - Hadoop敏感数据块防泄露
  - 数据库TDE防范库文件泄漏

【炼石方案举例】模式12案例-TFE透明文件加密



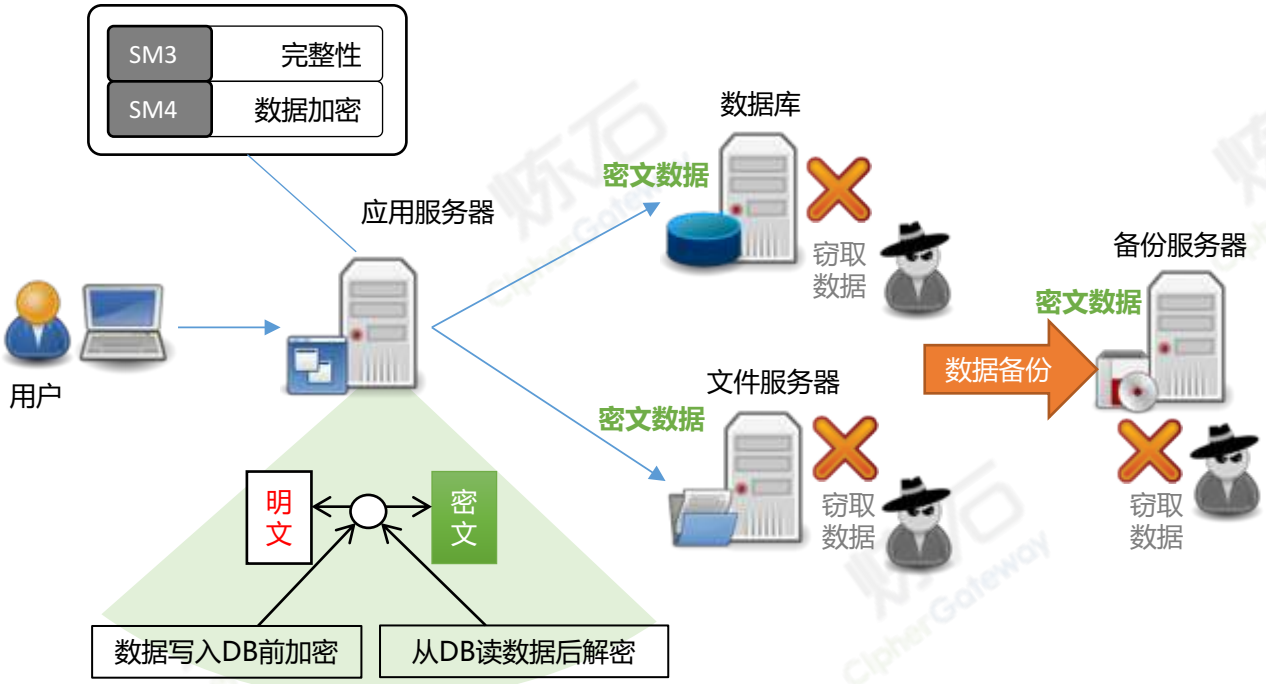
- 通过在Windows/Linux驱动层安装炼石TFE模块，应用免改造实现存盘文件密文存储。 TFE驱动模块与文件加密管理平台交互，获取加解密策略以及密钥。
- 可指定要加密的文件夹，该文件夹（及其子文件夹）的文件在保存时被加密，也可选择全盘加密；可选择要授权的应用，通过白名单机制使应用正常访问；而未授权应用或者直接拷贝文件，只能读取密文文件。
- 密钥生命周期管理平台统一进行加解密所使用密钥的管理工作。文件加密管理平台与密钥生命周期管理平台进行交互，获取加解密所使用的密钥。

模式13-应用内数据加密：威胁分析



- 威胁分析
  - 攻击者可以从数据库或文件服务器直接窃取敏感数据
- 环境/约束条件
  - 敏感数据可在应用内处理计算，或无需在数据库进行复杂计算
- 模式威胁示例
  - ERP中配方泄露
  - 业务系统中个人信息数据泄露

模式13-应用内数据加密：防护模型



- 解法
  - 在应用内节点加密数据，结合业务逻辑加密重要数据
- 关联解法
  - 数据库TDE加密：需要适配不同数据库及多版本
- 效果/注意点/副作用/局限性
  - 依赖于应用软件框架
  - 数据库无法对密文数据进行复杂计算
- 参考案例
  - ERP系统中配方数据防护
  - 业务应用系统对个人信息加密防护

【炼石方案举例】模式13案例-炼石CASB插件版实现用户与字段级细控

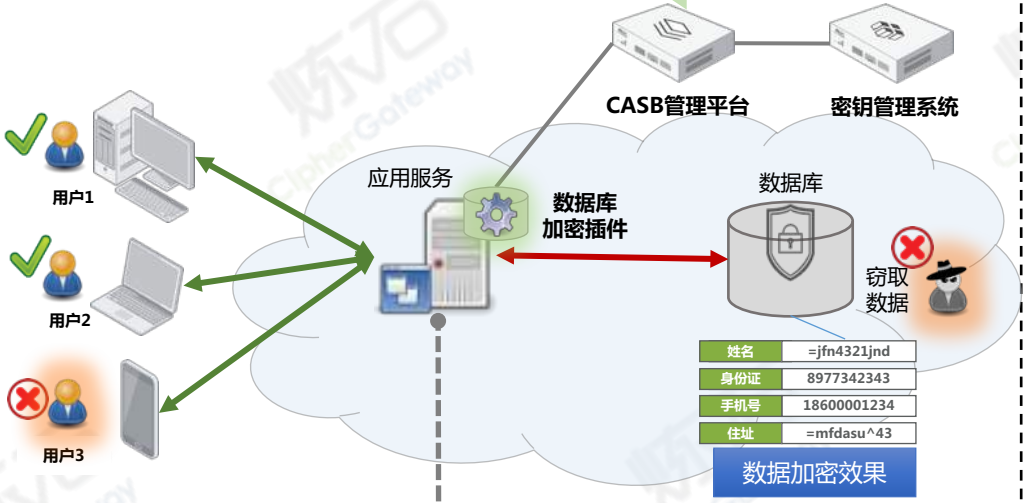
支持ABAC的访问控制策略，实现用户与字段文档级防护

动态脱敏效果

姓名	周林
身份证	62108756125
手机号	17712348471
住址	中关村大街

姓名	周林
身份证	6210****125
手机号	177****8471
住址	***大街

姓名	***
身份证	**********
手机号	**********
住址	**********



姓名	=jfn4321jnd
身份证	8977342343
手机号	18600001234
住址	=mfdasu^43

数据加密效果

数据发现：
- 元数据提取、数据扫描
- 特定数据发现（如个人信息）

数据加密：
- 字段或文档级加密
- 锚点解密的防绕过细控与审计

行为审计：
- 可定责的日志防篡改审计
- 数据访问风控

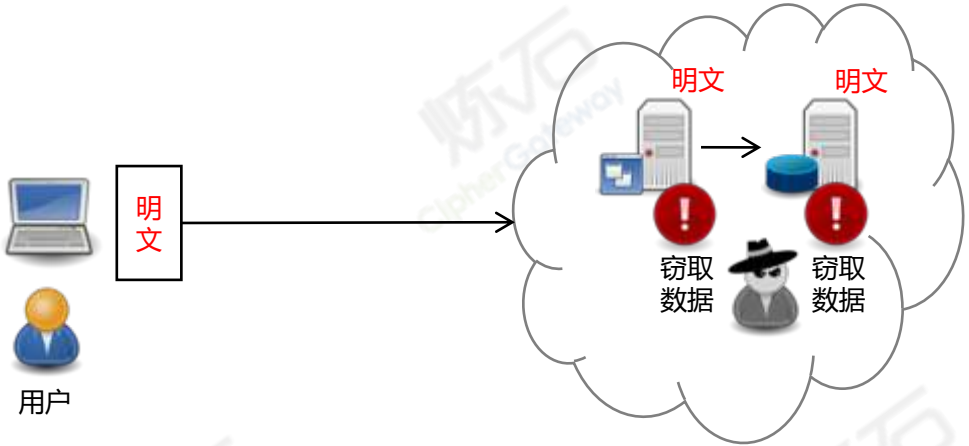
访问控制：
- 基于属性和角色的访问控制
- 丰富的数据脱敏策略

用户级细控的数据加密

【专利保护的技术创新】
- 应用侧插件对数据操作进行拦截和代理，实现入库数据加密与细控
- **Aspect Oriented Encryption**，面向切面加密防护
- **Critical Application Security Brokers**，CASB插件模式

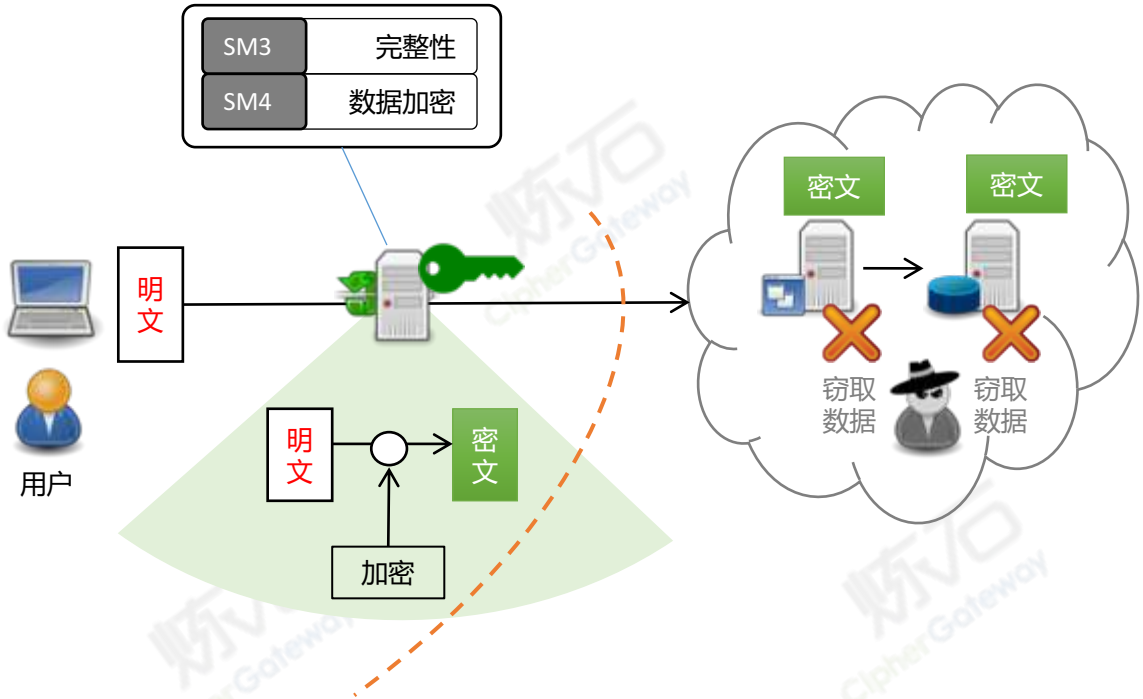
【技术优势】
- **免开发改造应用，敏捷实施**。只需部署“插件+盒子”即可实现字段级安全增强
- **支持各种数据库**。支持所有主流数据库，及其不同版本
- **防绕过的用户与字段级细控**。结合用户身份与业务上下文，将密码与细控及审计紧密结合，实现有效数据防护

模式14-业务数据代理网关加密：威胁分析



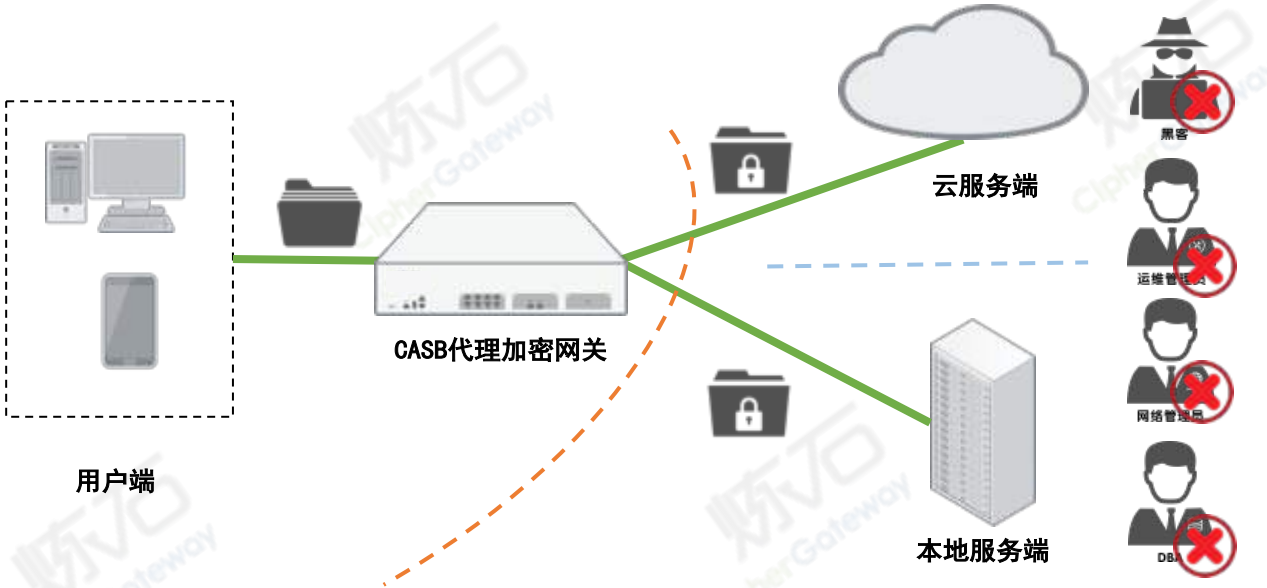
- 威胁分析
  - 敏感数据上传到云(或服务端)，云(或服务端)存在数据泄漏风险
- 环境/约束条件
  - 零信任环境的数据威胁
- 模式威胁示例
  - SaaS等云应用数据泄露
  - 本地服务端数据泄露

模式14-业务数据代理网关加密：防护模型

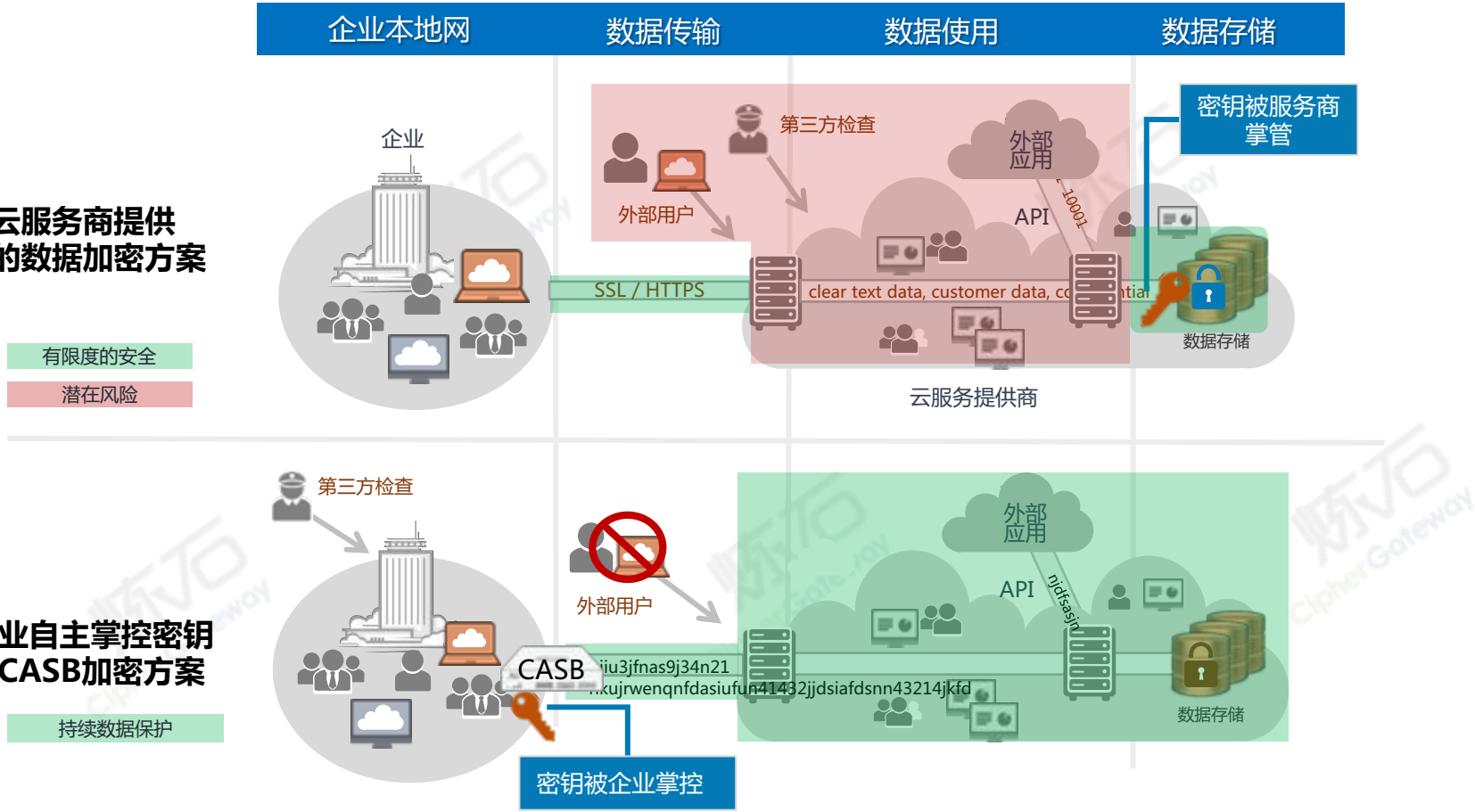


- 解法
  - 用户把数据提交给CASB产品，CASB识别数据格式，并对敏感数据加密后上传云(或服务端)
- 关联解法
  - 云(或服务端)的TDE+密钥管理
- 效果/注意点/副作用/局限性
  - 加密后数据计算通过可计算加密模型解决，成本较高但防护效果好
  - 优点是用户自己掌控密钥
- 参考案例
  - CASB加密保护上云敏感数据安全

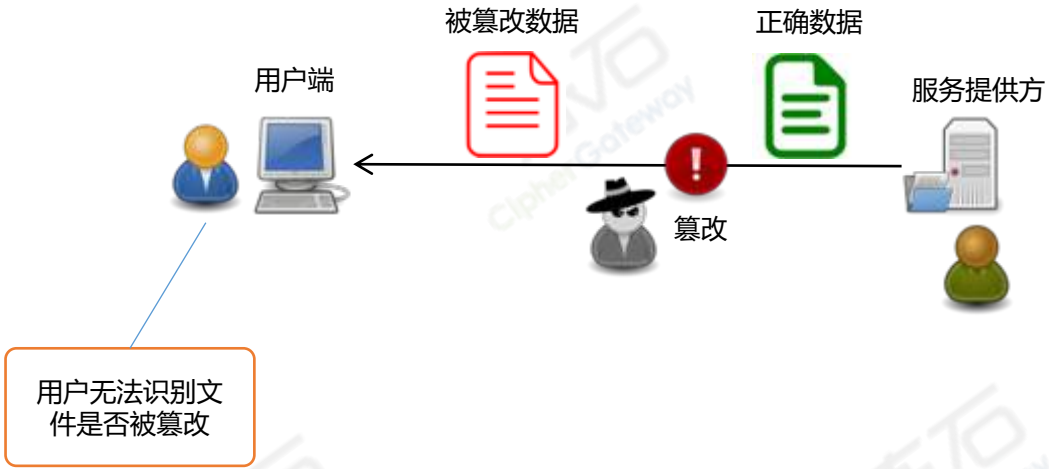
【炼石方案举例】模式14案例-CASB代理加密网关保护上云数据



模式14案例-云访问CASB让用户掌控密钥加密数据

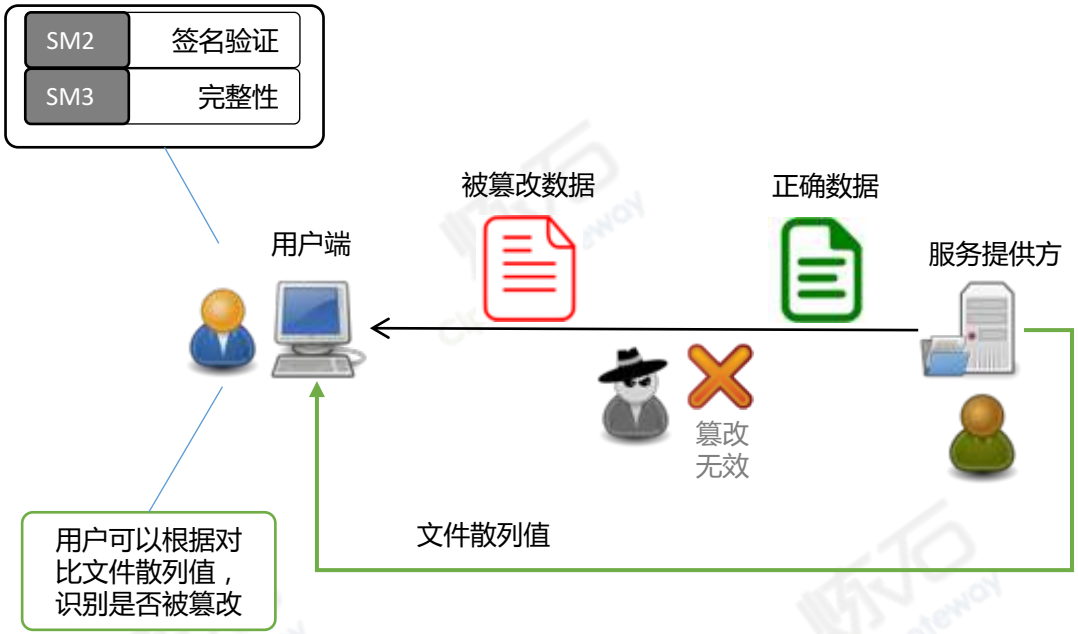


模式15-基于密码校验的防篡改：威胁分析



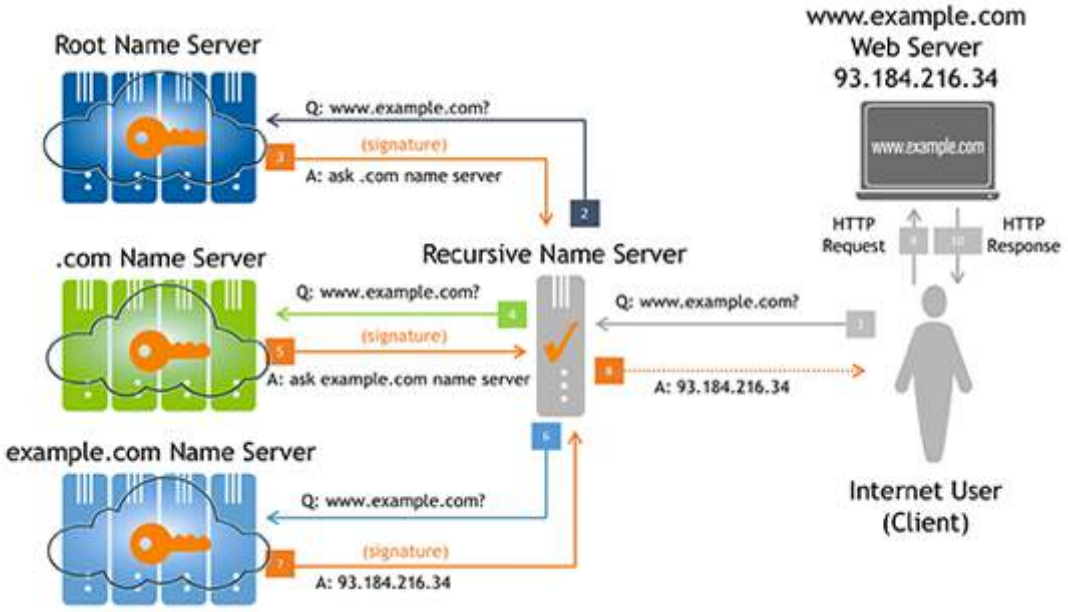
- 威胁分析
  - 【完整性】数据在分发过程中可能被篡改
- 环境/约束条件
  - 和原始数据获取相比，散列值获取有更安全的通道
- 模式威胁示例
  - 下载关键软件时内容被篡改

模式15-基于密码校验的防篡改：防护模型



- 解法
  - 用散列值校验数据完整性
- 关联解法
  - HMAC，但需要预共享密钥
- 效果/注意点/副作用/局限性
  - 散列值获取方式，要比数据更安全
- 参考案例
  - 用公钥验签技术防护DNS解析，保障DNS记录正确
  - 下载关键软件的散列值安全校验

模式15案例-用签名验证技术保护DNS记录防篡改

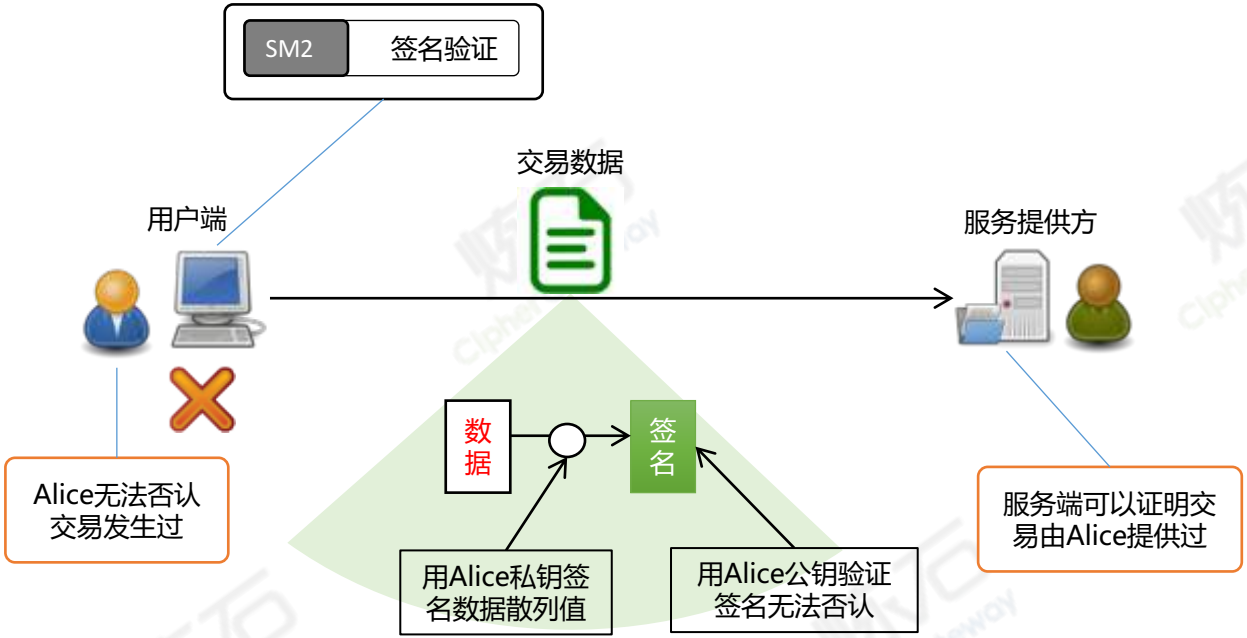


- DNSSEC（Domain Name System Security Extensions）是IETF对确保由DNS中提供的关于IP网络使用特定类型的信息规格包。
- DNSSEC对DNS提供给DNS客户端（Resolver）的DNS数据来源进行认证，并验证不存在性和校验数据完整性验证，但不提供或机密性和可用性。
- 目前仅部署在.org域名和.gov（美国政府域名）以及部分国家和地区顶级域（ccTLD）。
- 2010年7月18日，根域名服务器（root-servers.net）已经完成DNSSEC签名。

模式16-基于私钥签名的责任认定：威胁分析

- 威胁分析
  - 【不可否认性】保证某个操作是用户本人做过
- 环境/约束条件
  - 用户有自己的私钥
- 模式威胁示例
  - 网络操作无法明确发起防责任，比如网上签署合同

模式16-基于私钥签名的责任认定：防护模型

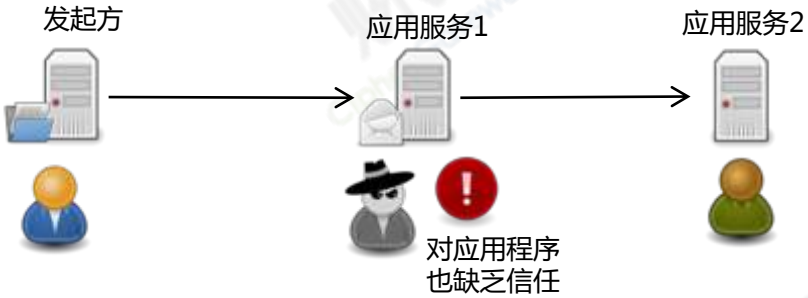


- 解法
  - 基于PKI的电子签章
- 关联解法
  - 纸质签字
- 效果/注意点/副作用/局限性
  - 私钥要无法被复制，并且用户能妥善保管
- 参考案例
  - 基于密码签名的电子签章系统，保障责任认定

模式16案例-基于私钥签名实现电子签章

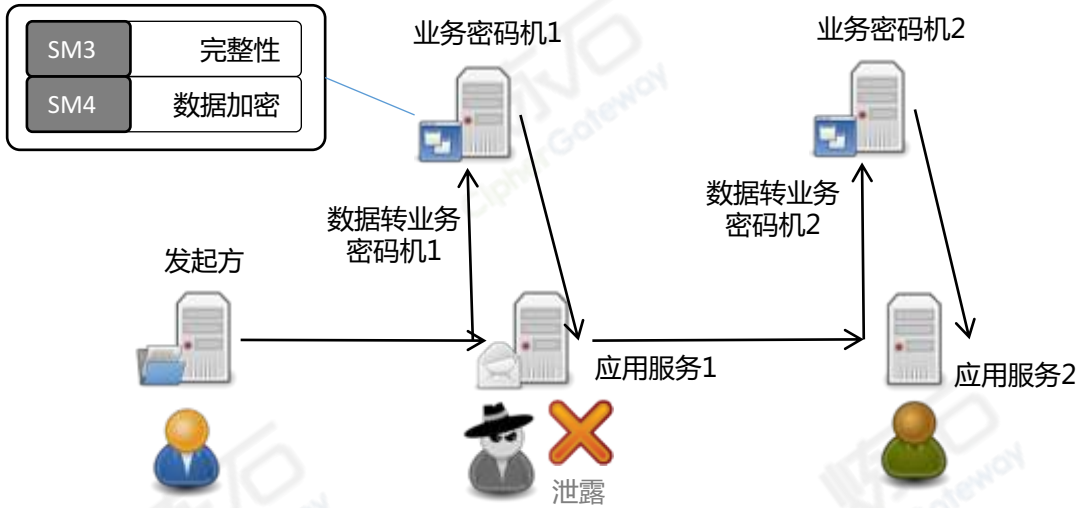
- 电子签章，与数字证书一样,是用来做为身份验证的一种手段，泛指所有以电子形式存在，依附在电子文件并与其逻辑关联，可用以辨识电子文件签署者身份，保证文件的完整性，并表示签署者同意电子文件所陈述事实的内容。
- 《中华人民共和国电子签名法》自2005年4月1日起施行。被称为“中国首部真正意义上的信息化法律”，自此电子签名与传统手写签名和盖章具有同等的法律效力。

模式17-灌装应用的密码机数据运算：威胁分析



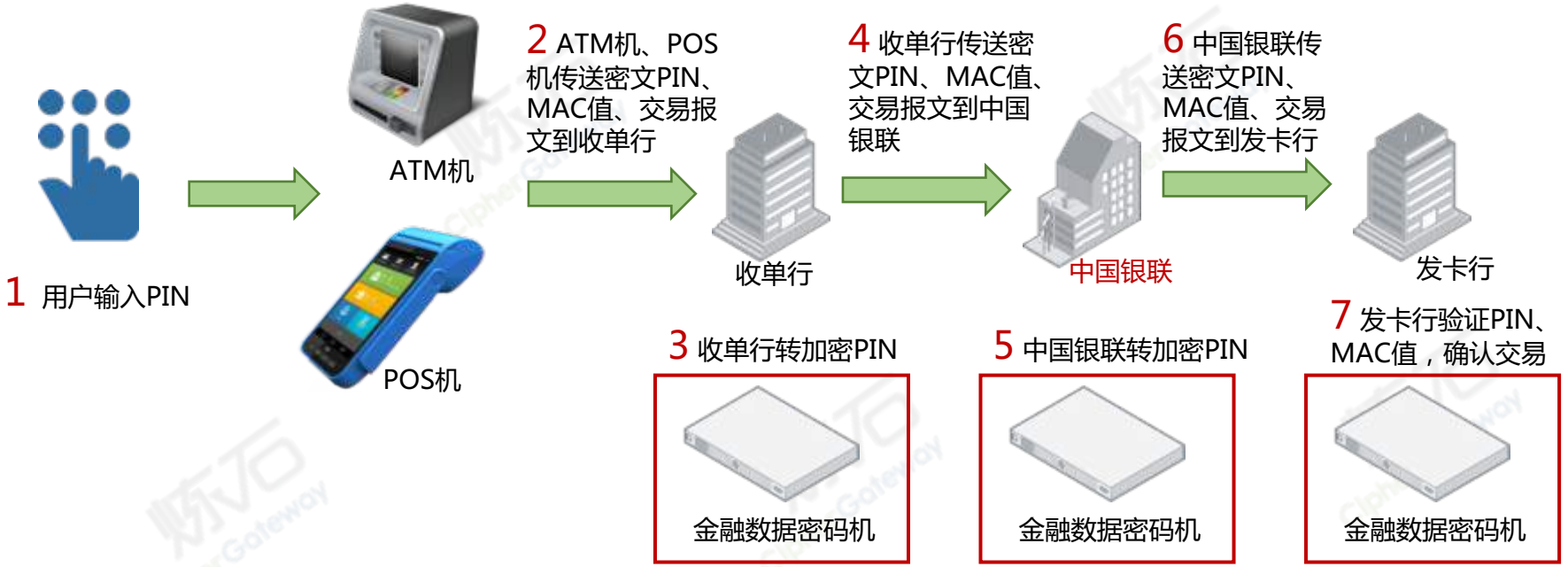
- 威胁分析
  - 数据在业务交换过程中，存在泄漏和篡改风险
- 环境/约束条件
  - 应用运行环境也存在风险，只有HSM能提供足够安全
- 模式威胁示例
  - 信用卡PIN码被泄露
  - 汇票密押被篡改

模式17-灌装应用的密码机数据运算：防护模型



- 解法
  - 预置密钥、灌装应用的专用密码机
- 关联解法
  - 应用服务器+密管系统
- 效果/注意点/副作用/局限性
  - 密码机预置密钥有成本，而且一旦丢失要求关联更换密钥
- 参考案例
  - 金融密码机采用定制HSM技术，防止潜在数据泄露和篡改风险
  - 密押系统防篡改

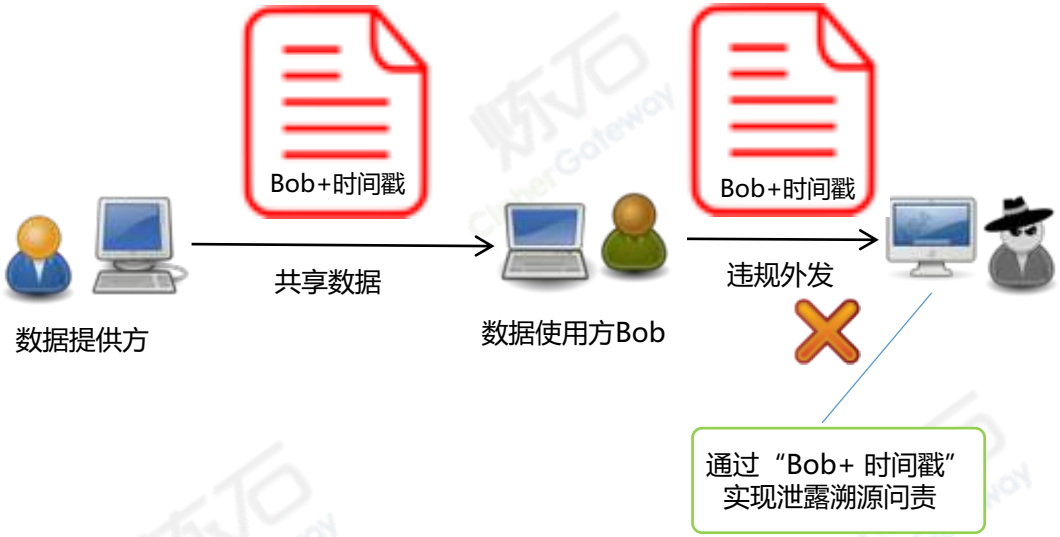
模式17案例-线下银行卡交易密码应用架构



模式18-基于数字水印加密的可追溯-威胁分析

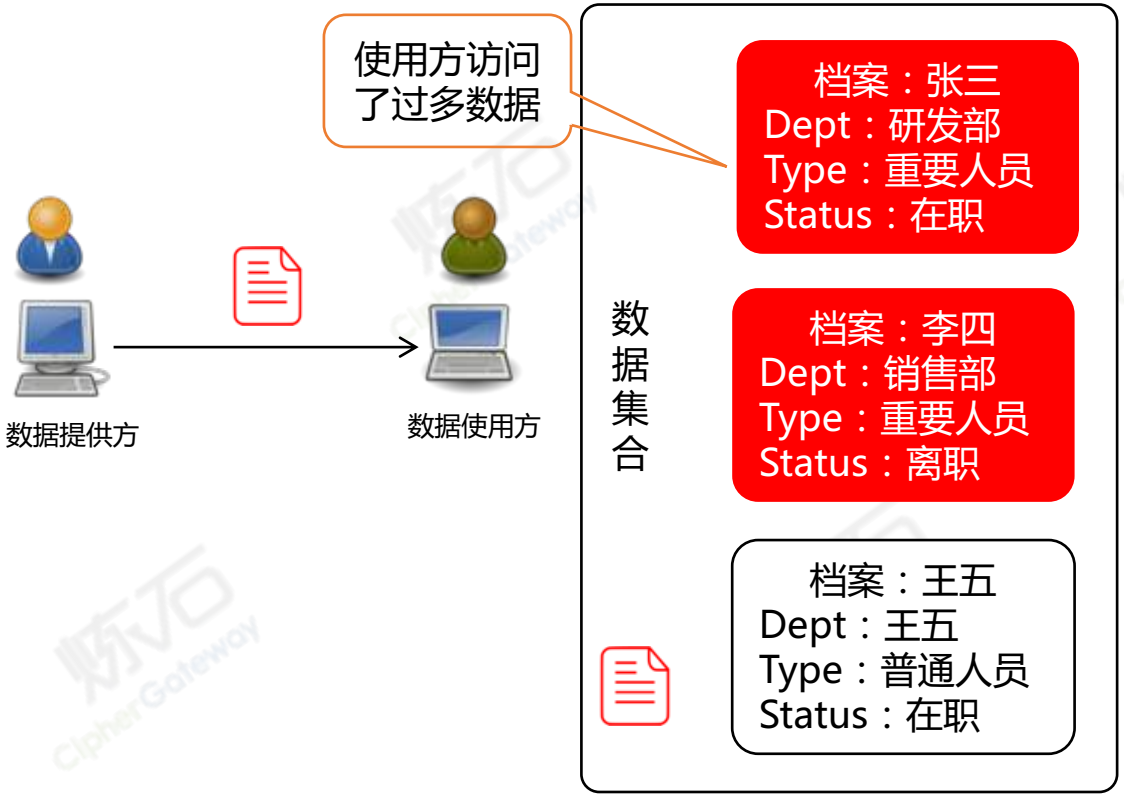
- 威胁分析
  - 数据违规外发（或泄露）后，无法追溯泄露源
- 环境/约束条件
  - 数据格式允许添加附加信息，通过可见水印、或不可见水印（隐写术）
- 模式威胁示例
  - 数据分享场景下违规外发
  - 数据泄露发生后的追溯问责

模式18-基于数字水印加密的可追溯-防护模型



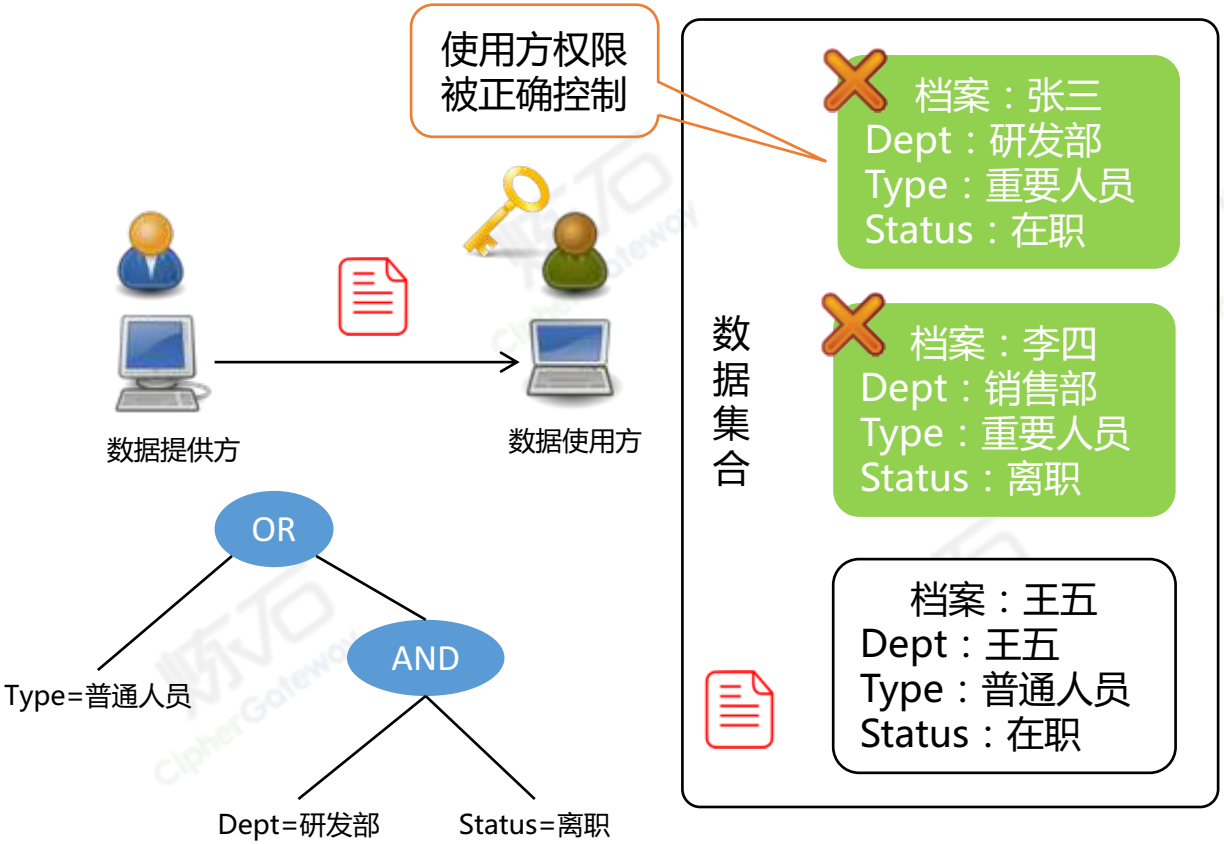
- 解法
  - 基于密码技术的数字水印
- 关联解法
  - TDF技术
- 效果/注意点/副作用/局限性
  - 存在水印信息被擦除的风险
  - 结构化数据难以添加水印
- 参考案例
  - 对外发图片、文档添加水印

模式19-基于属性加密的访问控制-威胁分析



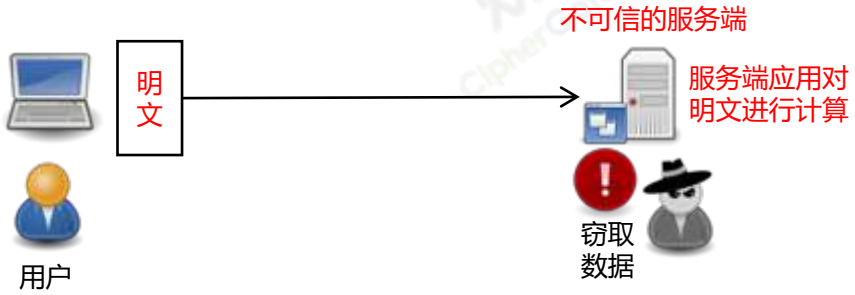
- 威胁分析
  - 数据使用方权限过大，对数据可以不受限的访问
- 环境/约束条件
  - 数据集合包含了不同的属性，数据使用方根据属性拥有不同密钥
- 模式威胁示例
  - 数据分享场景下滥用数据

模式19-基于属性加密的访问控制-防护模型



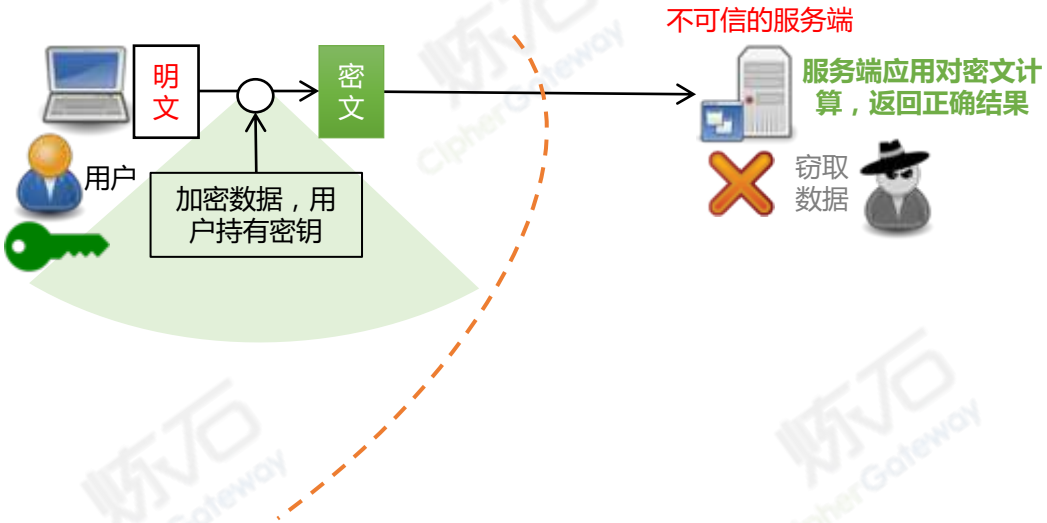
- 解法
  - 基于ABE的细粒度访问控制
- 关联解法
  - 数据外发时脱敏
- 效果/注意点/副作用/局限性
  - 数据使用方要具备细粒度秘钥信息
- 参考案例
  - 基于ABE的云端数据共享

模式20-不可信环境中的数据运算：威胁分析



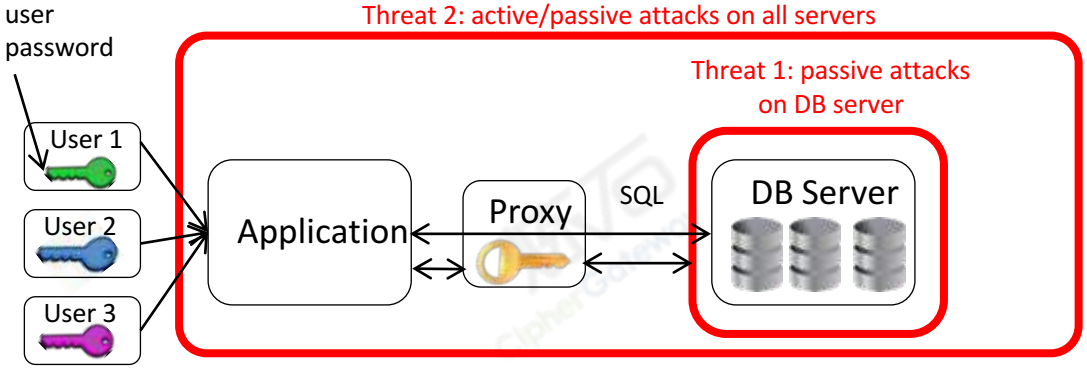
- 威胁分析
  - 服务端不可信，但需要把数据交付服务端进行计算
- 环境/约束条件
  - 不可信环境下提交数据进行计算
- 模式威胁示例
  - 云端对敏感数据计算

模式20-不可信环境中的数据运算：防护模型

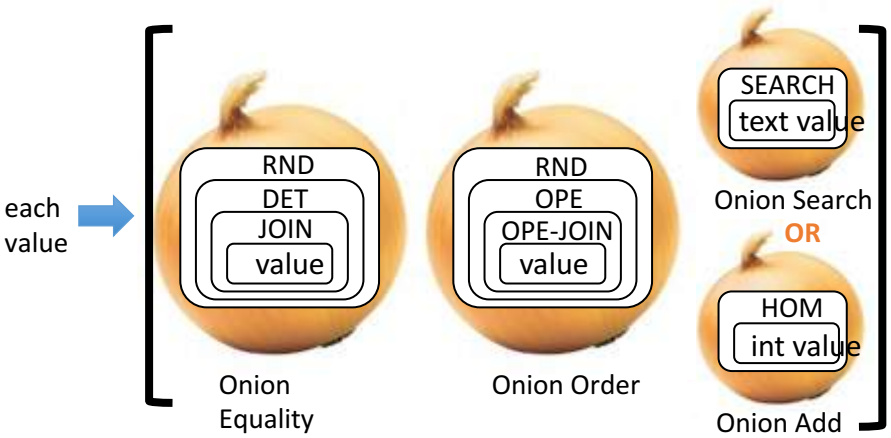


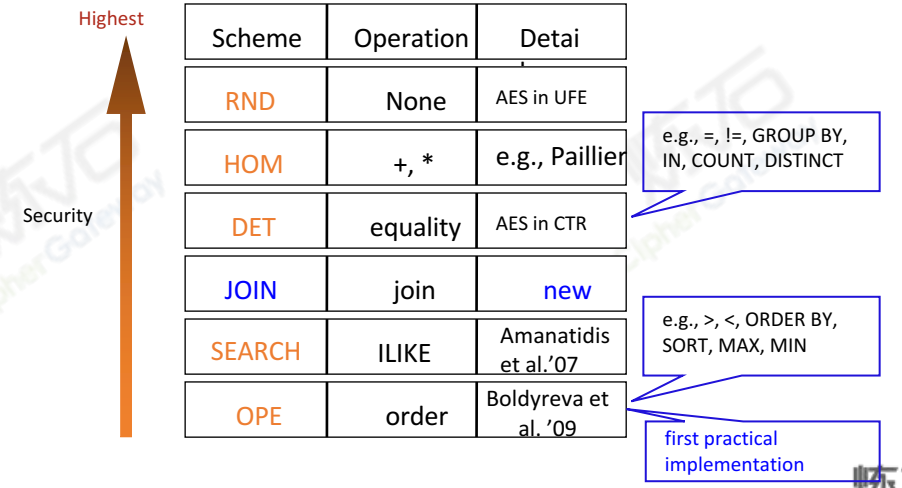
- 解法
  - 同态加密、MPC多方计算、零知识证明等隐私计算技术
- 关联解法
  - 用户掌控证明的SGX等服务端可信技术
- 效果/注意点/副作用/局限性
  - 目前同态加密效率低，并且效率改进与高安全性无法兼得
- 参考案例
  - 基于同态加密的数据库加密网关，防范服务端威胁

模式20案例-用同态加密实现不可信服务端的数据运算

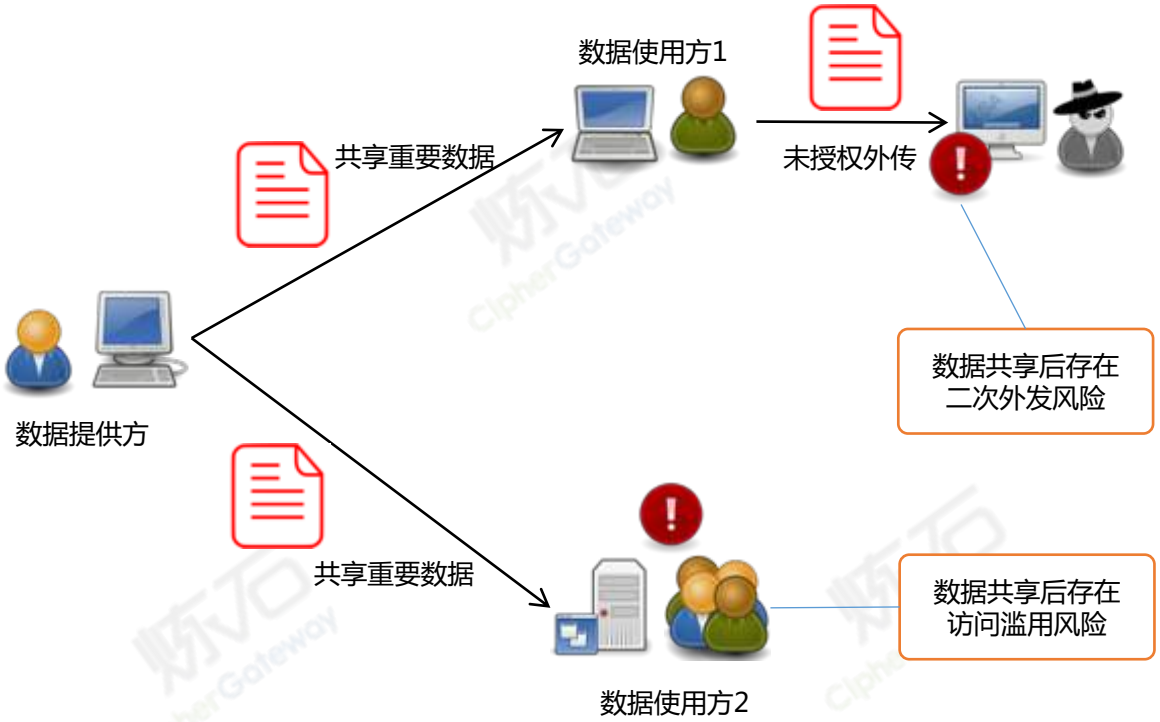


- CryptDB是MIT的开源项目，支持MySQL，部署在应用服务器和数据库服务器之间，实现数据库透明加密网关
- 采用洋葱加密模型实现MySQL的可计算密文，需要在MySQL安装UDF插件。
- 服务端数字计算采用了同态加密



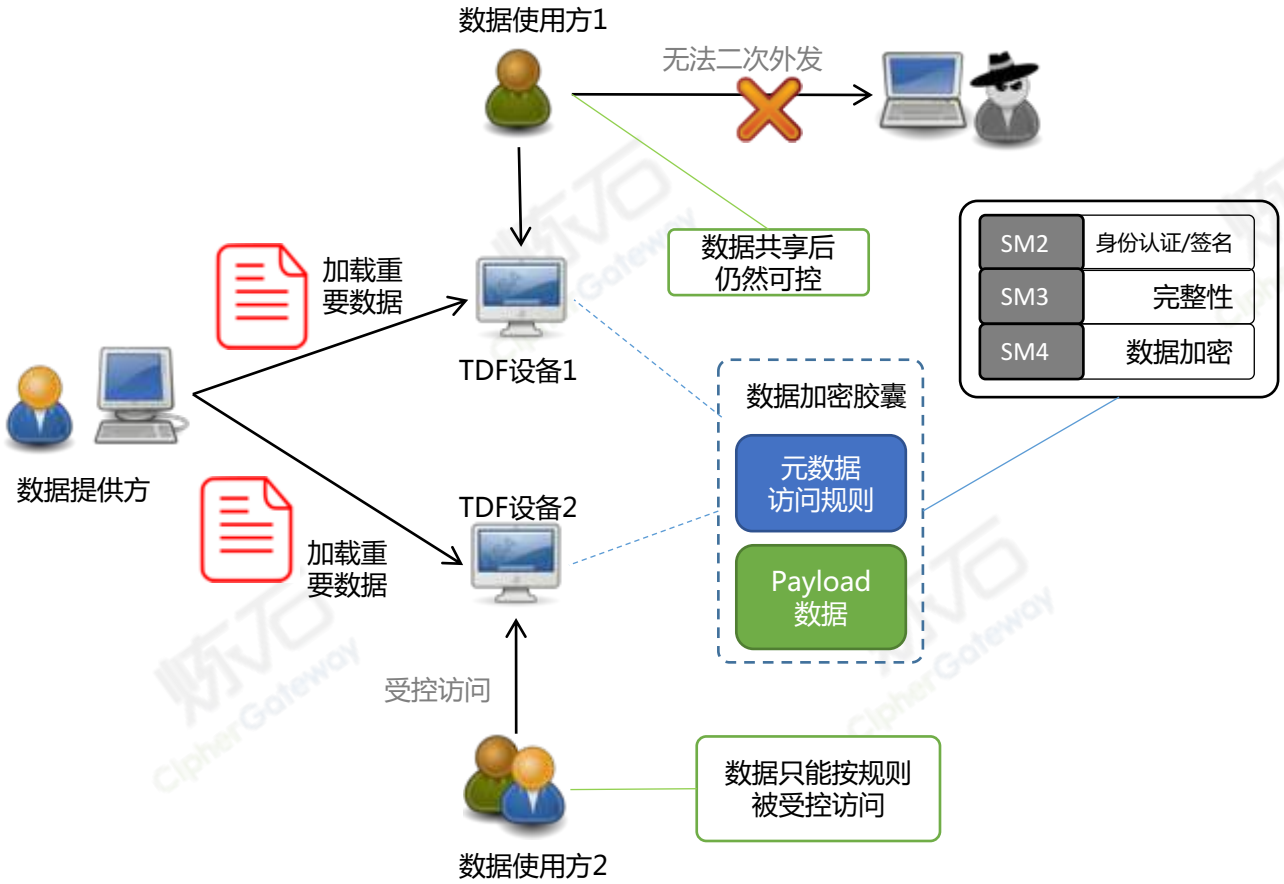


模式21-基于TDF的可控分享秘密信息：威胁分析



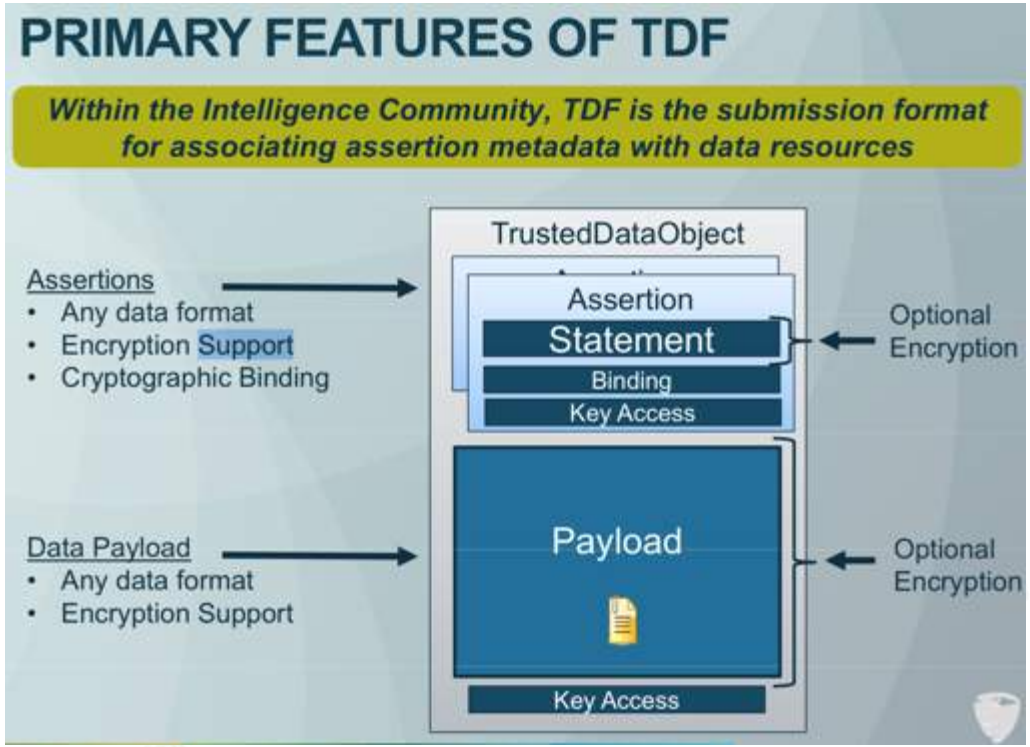
- 威胁分析
  - 数据在流动中可以轻易复制访问滥用、甚至未授权二次外发，授予数据访问权带来了所有权失控
- 环境/约束条件
  - 数据不得不共享，但共享后不再受控
- 模式威胁示例
  - 商业秘密数据分享失控
  - 跨组织分享敏感数据被滥用

模式21-基于TDF的可控分享秘密信息：防护模型



- 解法
  - 基于密码技术实现数据管控，专用设备安全堡垒进一步使数据共享受控
- 关联解法
  - 不共享数据：业务停滞
  - 开放数据：风险失控
  - 数据脱敏：业务受阻
- 效果/注意点/副作用/局限性
  - TDF实施和使用成本较高
  - 专用共享设备安全增强
- 参考案例
  - 美国情报体系用IC-TDF保护国家机密安全共享

模式21案例-美国情报体系使用TDF分享机密数据

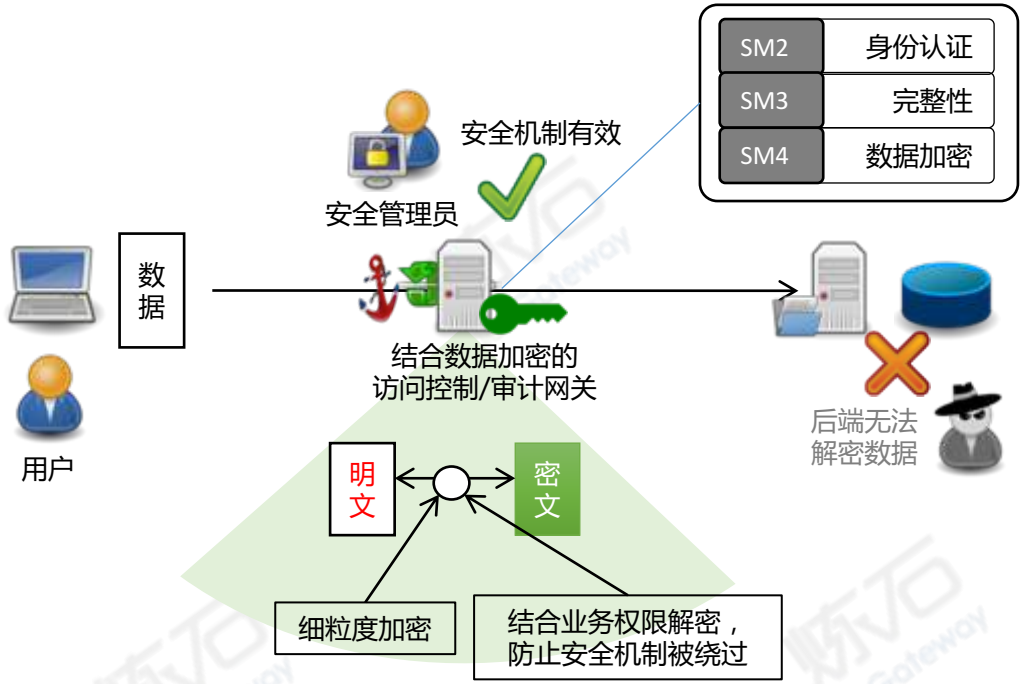


- TDF(可信数据格式)是一种数据对象编码规范，用于启用数据标记和加密安全功能。
- 美国情报部门维护IC-TDF，用于美国16个情报组织间的机密数据交换，达到美国高价值情报数据的高效、安全共享流转。

模式22-锚点解密的防绕过数据安全：威胁分析

- 威胁分析
  - 数据在服务端可直接窃取，访问控制可以被绕过，同时审计置信度较低
  - 这既会带来数据威胁，也是对安全机制本身的破坏
- 环境/约束条件
  - 数据是流动的，缺乏一个数据集中控制点
- 模式威胁示例
  - 应用-数据库模式下，存在应用外数据访问，比如DBA窃取
  - 数据共享场景下的数据流转

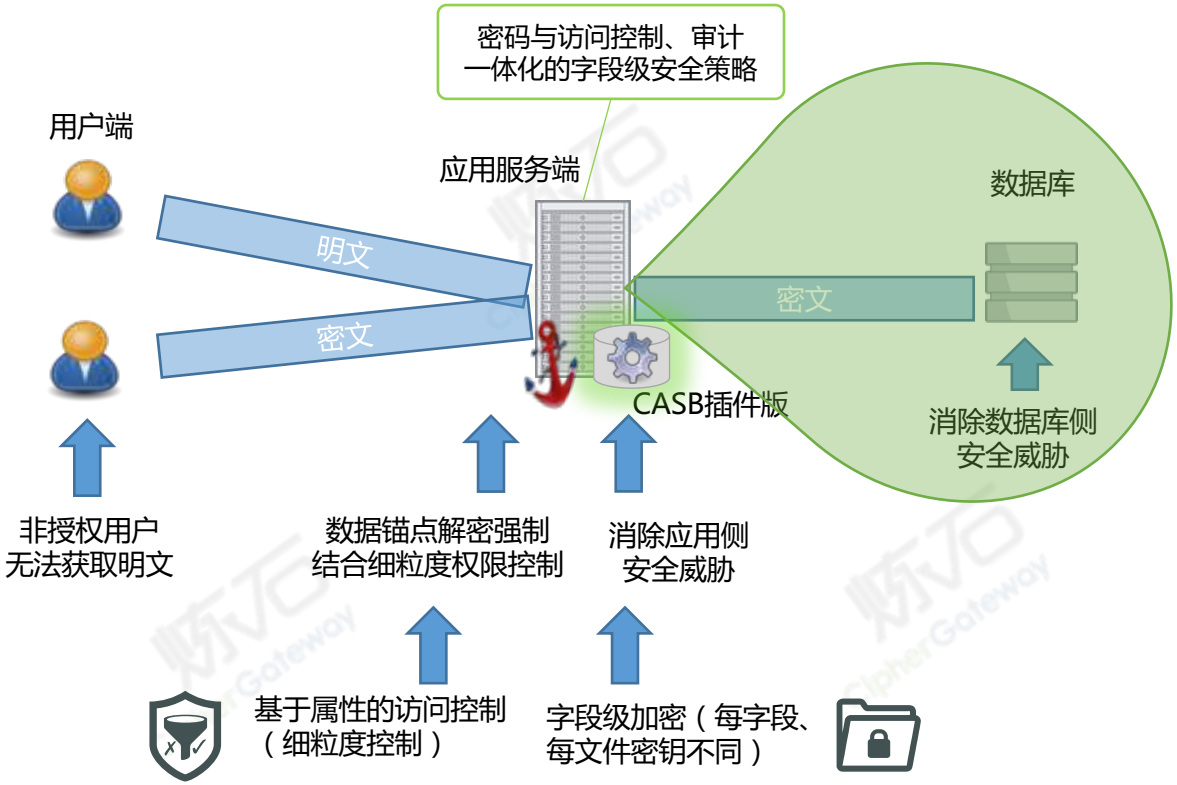
模式22-锚点解密的防绕过数据安全：防护模型



- 解法
  - 用加密构建一个数据的集中控制点，在该控制点进行细控，并留存日志提供高置信度审计
- 关联解法
  - 直接用访问控制和审计，但存在“马其诺防线”被绕过
- 效果/注意点/副作用/局限性
  - 缺点是复杂数据加密后对计算有影响，因此需要结合业务使用，适用于重要数据
- 参考案例
  - 企业应用CASB实现防绕过的安全机制

以密码为核心、细控和审计等安全技术互相融合！

【炼石方案举例】模式22案例-密码控审一体化，安全机制防绕过



【密码提供的安全价值】

- 消息安全性等同于密钥安全性
  - 密钥安全性可扩大为消息安全性
  - 密钥不安全可扩大为消息不安全
  - 数据很大，但密钥很小
- 将安全问题缩小到密钥管理问题
- 将密钥管理与访问控制、审计结合，构建“防绕过”的数据安全防线

关于我们—北京炼石网络技术有限公司

炼石 CipherGateway

CG Lab

- 基于CASB与密码技术的新一代数据安全解决方案提供商， 获多轮投资；
- 创新CASB插件模式免改造应用增强安全；PCT专利保护最快国密实现；
- 团队精通密码工程化、应用重构优化，擅长应用安全增强与国密改造；

- 愿景：成为最有价值的数据安全公司
- 使命：将安全适配进应用，让数据共享更有价值

- CipherGateway-应用免改造的数据安全产品
  - CASB插件版-用户与字段级加密细控，数据共享与安全兼得
  - CASB代理网关版-业务上下文安全防护，增强应用的安全能力
  - CASB公有云版-云端数据风险管控，增强对云的信任
- CipherSuite-高性能基础密码产品
  - 高性能服务器密码机、专业KLM密钥生命周期管理系统
  - 高效、安全、易用、场景覆盖全面的密码SDK

炼石
CipherGateway

谢谢！