北京江南天安科技有限公司
商用密码技术在等级保护建设中的最佳实践

2019年1月18日

www.tass.com.cn

CONTENTS

目 录

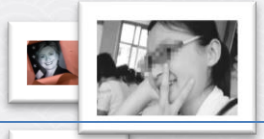
一 信息安全态势

Anywhere
Anytime
Anydevice

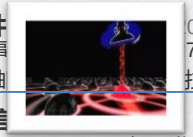
VS

Anywhere
Anytime
Anydevice

网络安全事件在全球泛滥



希拉里‘邮件门’事件(2015.3)
- 2015年3月，邮件门事
- 10.28，FBI重启对“邮
- 7晚，“维基揭秘”再爆“猛料”；
- 拉里大选失败。

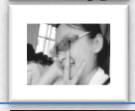


惊曝淘宝9900万账户信
- 10月14日至16日通过租用阿里云服务器进行“撞库”；
- 利用手中已有非淘宝账号对淘宝网进行了9900多万次比对，用于抢单等。

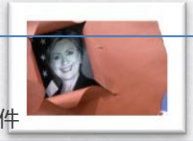
Facebook爆出史上最大数据泄露丑闻

徐玉玉事件

惊曝淘宝9900万账户信息遭窃



徐玉玉事件成电信诈骗之殇(2016. 8)
- 黑客入侵“山东省2016高考网上报名信息系统”，60多万条信息泄露；
- 助学金诈骗，导致徐玉玉死亡。



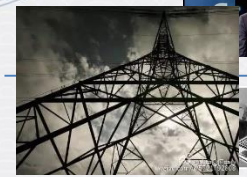
乌克兰70万家庭断电(2016. 12)
- 这是世界上首例由恶意软件而引发
- 一封针对性的钓鱼邮件，攻击者
- 件。
- 员工，并引诱其点击恶意软件

勒索病毒“永恒之蓝”席卷全球(2
- 2017年5月12日，一种名为WannaCry的勒索病毒肆虐，造成英国、俄罗斯
- 以及
- 的多个高校校内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金才能解密恢复文件。

“黑客”入侵快递公司后台盗近亿客户信息　“勒索病毒”“永恒之蓝”

希拉里‘邮件门’

比勒索病毒更恐怖的“永恒之石”来了！(2017. 5)
- 2017年5月24日，勒索病毒WannaCry的余波未消，更恐怖的新病毒已经出现了。相比WannaCry，这个名叫EternalRocks（永恒之石）的新病毒更加让人胆寒。



Facebook　　泄露丑闻，数据帝国崩解危机引爆(2018. 3)
- 2018年3　　斤公司剑桥分析（Cambridge Analytica) 在未经用户许可的情况下，盗用了
- 千万用户　　分析预测，并涉嫌以此进行社交媒体操作影响大选中的选民行为。

“黑客”入侵快递公司后台盗近亿客户信息(2018. 5)
- 　　案，杨某、胡某、陈某因犯侵犯公民个人信息罪均被判处3年以上有期徒刑，并处罚金。

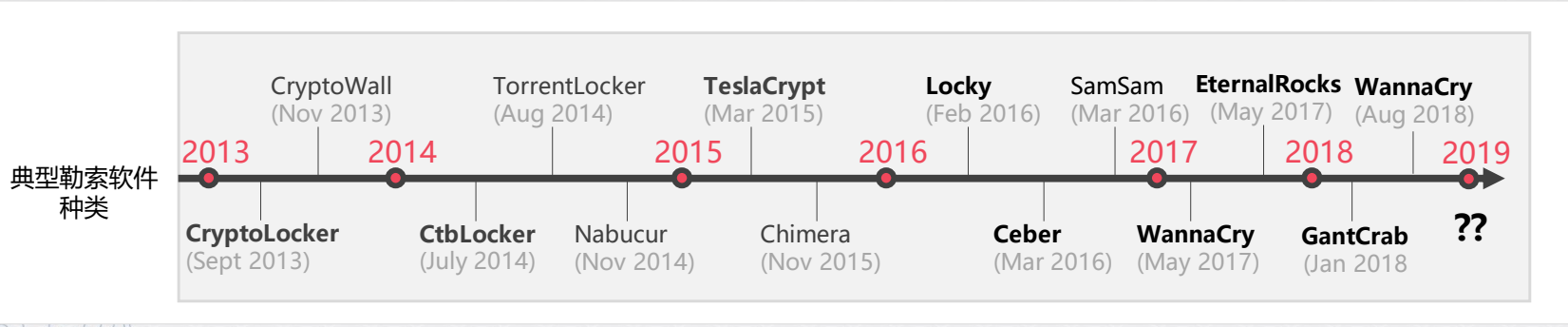
比勒索病毒更恐怖的“永恒之石”来了

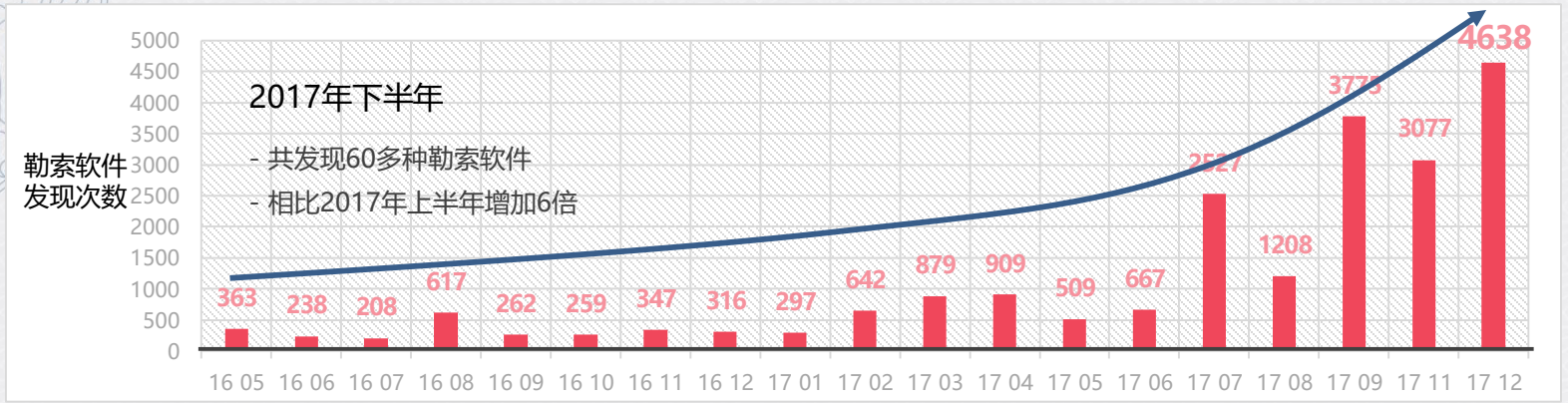
万豪5亿客户信息泄露给了谁当头一棒？

乌克兰70万家庭断电

万豪5亿客户信息泄露 给了谁当头一棒？(2018. 11)
- 2018年11月19日万豪国际调查发现，2018年9月10日继之前喜达屋旗下酒店预订数据库中的宾客信息曾在未经授权的情况下被访问，而这其中涉及到在喜达屋酒店预订的约5亿名客人的信息。

近期信息安全事件——勒索软件





信息安全事件特点

威胁形式

- 利用无线和移动设备的攻击
- 利用侧道攻击
- 利用物联网攻击
- 利用邮件系统
- 利用电网系统
- 利用医疗系统
- 利用工业控制系统

目的

- 信息窃取
- 敲诈勒索
- 破坏国家基础设施

二 国家信息安全举措

国家高度重视信息安全

- 2014年2月，中共中央网络安全和信息化小组成立。
- 习主席“2.27讲话”：
  没有网络安全，就没有国家安全，没有信息化就没有现代化。
  网络安全和信息化是一体之两翼、驱动之双轮，
  必须统一谋划、统一部署、统一推进、统一实施。
- 2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》。
- 2017年6月1日，**《中华人民共和国网络安全法》**正式施行 。
- 2018年11月3日，**《信息安全技术 网络安全等级保护基本要求》**形成报批稿。

习近平在网络安全与信息化工作座谈会上的讲话

信息技术变化越来越快，过去分散独立的网络变得高度关联、相互依赖，网络安全的威胁来源和攻击手段不断变化，**那种依靠装几个安全设备和安全软件就想永保安全的想法已不合时宜，需要树立动态、综合的防护理念。**

金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。……**我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。**

（要）**全天候全方位感知网络安全态势。**知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。

要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。

关键安全预防措施

加强网络入侵防护

■关键基础设施一旦被入侵，危害极大，要重点进行网络入侵的防护。

■对于**传统威胁**，要做到快速、精准的防护；对于**高级未知威胁**，也要做到智能检测与防护。

■综上，建设和加强入侵防护是网络安全防护的**核心关键工作**

建设安全态势平台

■维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。

■综上，感知网络安全态势是网络安防护中**最基本、最基础的工作**




推广密码应用实现数据安全、网络安全和国家安全

安全职责所在

1. 以密码技术保证信息的机密、真实、完整、不可否认，是实现数据安全的主要手段；
2. 各行各业信息系统存储和传输的大量数据，亟待采用密码技术，实现业务效率与安全兼得。

严峻形势所迫

1. 关系国计民生、国家安全的广泛行业信息化系统，密码应用严重缺失；
2. 网络安全形势严峻。

政治责任所系

1. 国外密码存在安全风险；
2. 密码作为战略性资源和重要核心技术，不能受制于人，必须发展自主可控。

当今时代所需

1. 现有信息系统中广泛确实密码安全能力；
2. 国外密码算法占据大部分市场份额；
3. 用户迫切需要高质量自主密码产品。

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。

——习主席2018年4月在全国网络安全和信息化工作会议讲话

密码作为网络安全的核心技术，是保护国家安全和根本利益的战略性资源。

——栗战书2017年3月在密码应用工作会议讲话

国家密集颁布法律法规，推广密码保护重要数据

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，并开展商用密码应用安全性评估试点工作。

2018年6月

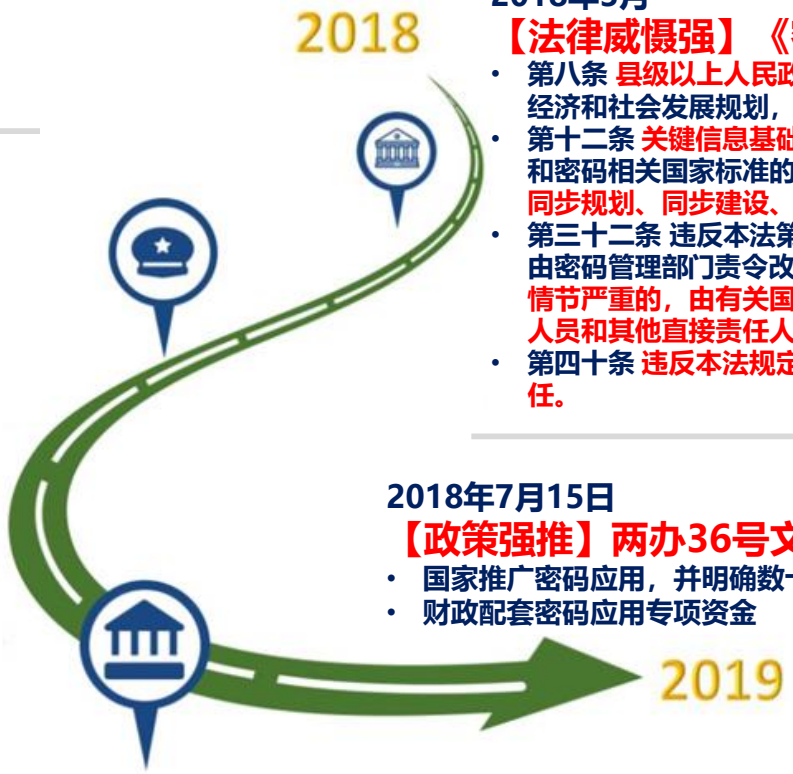
【抓手增强】公安部《网络安全等级保护条例》

- 第四十七条【非涉密网络密码保护】第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。

2018年7月

【抓手增强】网信办《关键信息基础设施安全保护条例》

- 第五十三条 关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。



2018年3月

【法律威慑强】《密码法》人大立法计划

- 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。

2018年7月15日

【政策强推】两办36号文

- 国家推广密码应用，并明确数十个部委任务
- 财政配套密码应用专项资金

三 国家对密码技术应用的要求

网络安全法对密码技术的要求

- 第三章 网络运行安全
  - 第一节 一般规定
    - 第二十一条 国家实行网络安全等级保护制度。
      - （四）采取数据分类、重要数据备份和**加密**等措施；
- 第四章 网络信息安全
  - 第四十条 网络运营者应当对其收集的**用户信息**严格**保密**，并建立健全用户信息保护制度。

网络安全等级保护对密码技术的要求——以三级系统安全通用要求为例

- 在基本要求中，在
  1. **通信传输**
  2. **身份鉴别**
  3. **数据完整性**
  4. **数据保密性**
  5. **安全方案设计**
  6. **产品采购和使用**
  7. **测试验收**
  8. **密码管理**
- 等8个控制点中的12个要求项提到密码技术的要求；

8.1.2.2 通信传输

a) 应采用校验技术或**密码技术**保证通信过程中数据的**完整性**；

8.1.4.1 身份鉴别

d) 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

8.1.4.7 数据完整性

a)应采用校验技术或**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

8.1.4.8 数据保密性

a)应采用**密码技术**保证重要数据在传输过程中的保密性，包括但不限于**鉴别数据**、**重**

8.1.9.2 安全方案设计

b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，**设计内容应包含密码技术**相关内容，并形成配套文件；

8.1.9.3 产品采购和使用

b) 应确保**密码产品与服务**的采购和使用**符合国家密码管理主管部门的要求**；

8.1.9.7 测试验收

b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告**应包含密码应用安全性测试相关**

8.1.10.9 密码管理

a) 应遵循**密码**相关国家标准和行业标准；

b) 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**。

网络安全等级保护对密码技术的要求——以三级系统安全通用要求为例

- 在安全设计技术要求中，在
  - **安全计算环境设计技术要求**
  - **安全通信网络设计技术要求**
- 中的**5**个要求项提到密码技术的要求；

7.3.1 安全计算环境设计技术要求

e) 用户数据完整性保护

应采用**密码等技术**支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

f) 用户数据保密性保护

应采用**密码等技术**支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

7.3.3 安全通信网络设计技术要求

b) 通信网络数据传输完整性保护

应采用由**密码等技术**支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

c) 通信网络数据传输保密性保护

应采用由**密码等技术**支持的保密性保护机制，以实现通信网络数据传输保密性保护。

d) 通信网络可信接入保护

可采用由**密码等技术**支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

第二章　密码应用

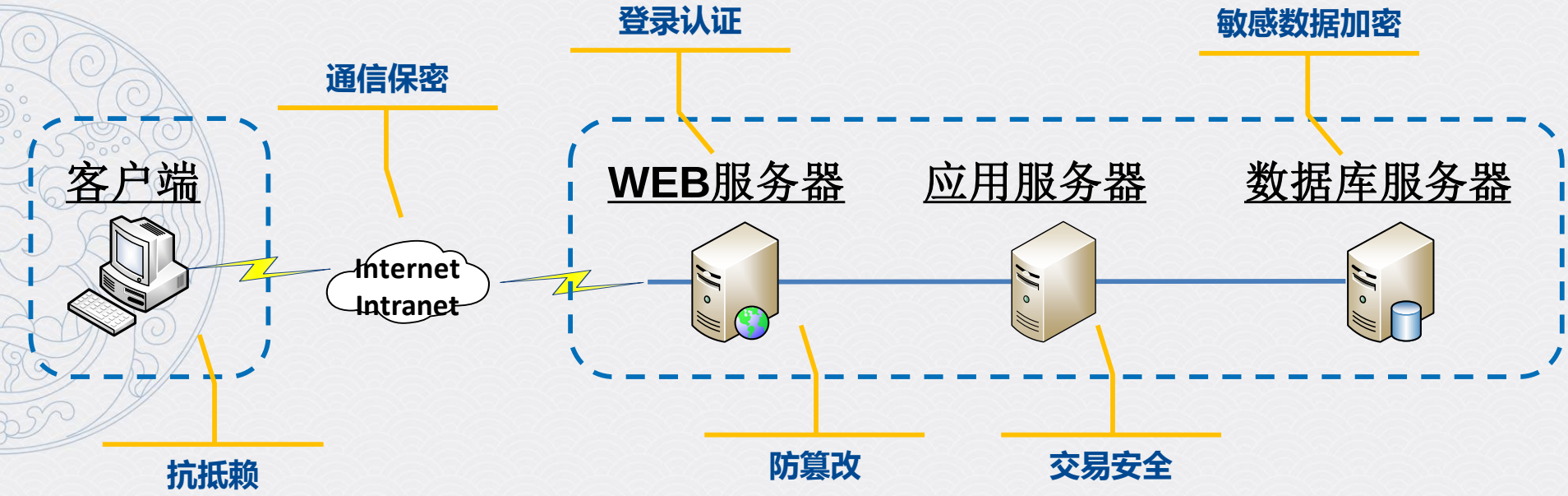
- 第十条　核心密码、普通密码可以用于保护国家秘密信息。**商用密码**用于保护不属于国家秘密的信息。

- 第十一条　国家密码管理部门对销售或者在经营活动中使用的商用密码产品，以及从事商用密码服务的**机构实施许可**。**商用密码产品**、**服务管理目录**由**国家密码管理部门**制定并公布。

- 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。

四 密码技术在信息安全工作中的应用

应用系统密码技术应用环节



应用系统密码技术应用案例——用户统一身份管理应用

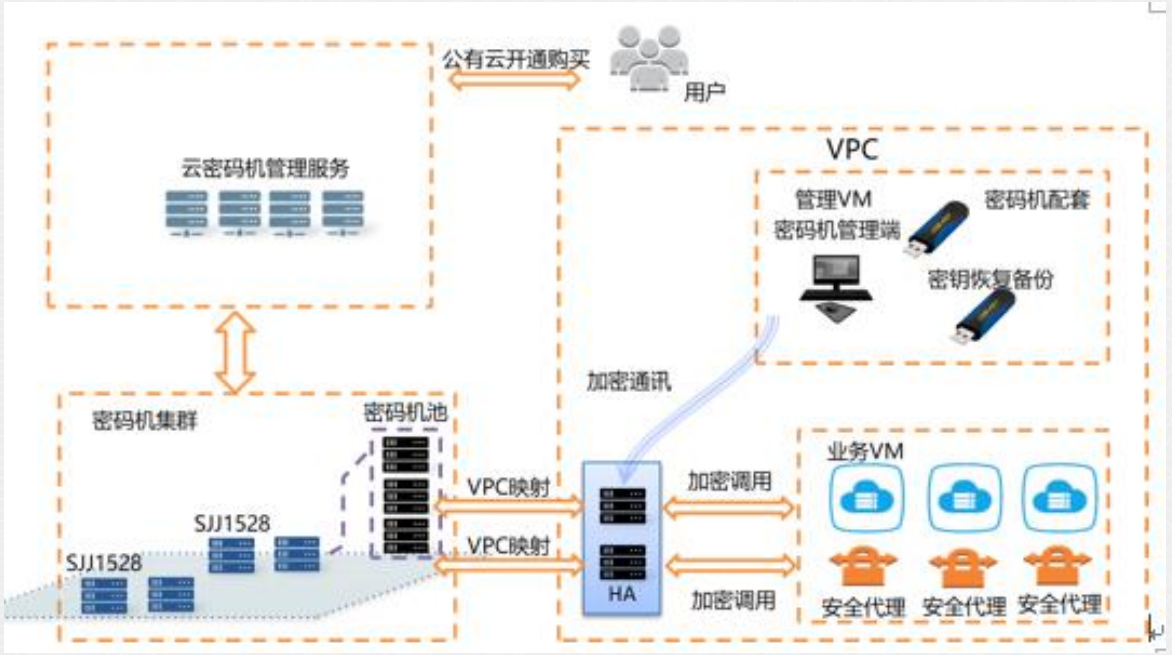
1. 人员登录信息系统的统一管理；
2. 建立应用系统集中登录平台；
3. 防止弱口令；
4. 满足等保三级关于登录信息系统的要求；
5. 符合国家关于国密算法的要求。

应用系统密码技术应用案例——公有云应用

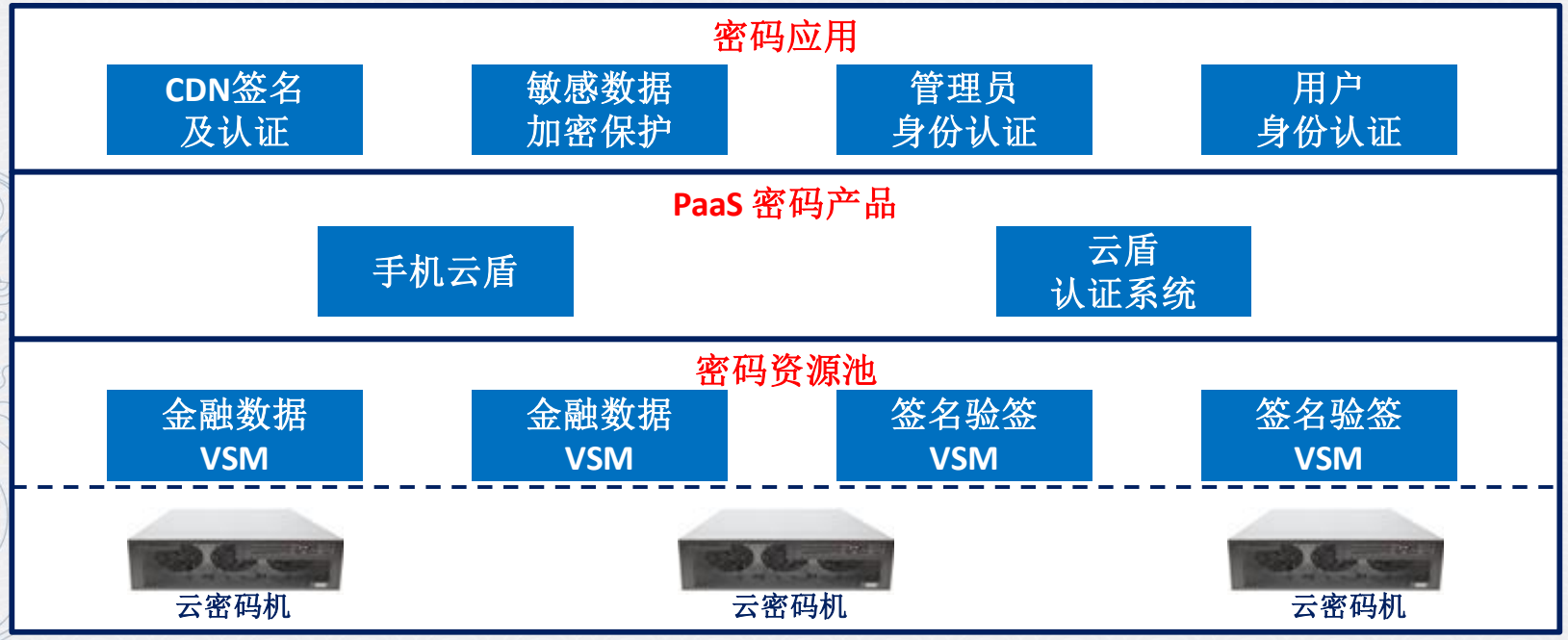
1. 2015年阿里云联合江南天安发布了公有云上第一个加密服务；

2. 为云用户提供数据加密功能；

3. 后续落地国内主流云服务商。



应用系统密码技术应用案例——政务云/专有云应用



1. 基于江南天安SJJ1528云密码机打造密码服务资源池；
2. 为手机应用提供安全的保护；
3. 防止弱口令；
4. 防止数据被篡改。

应用系统密码技术应用案例——金融行业应用

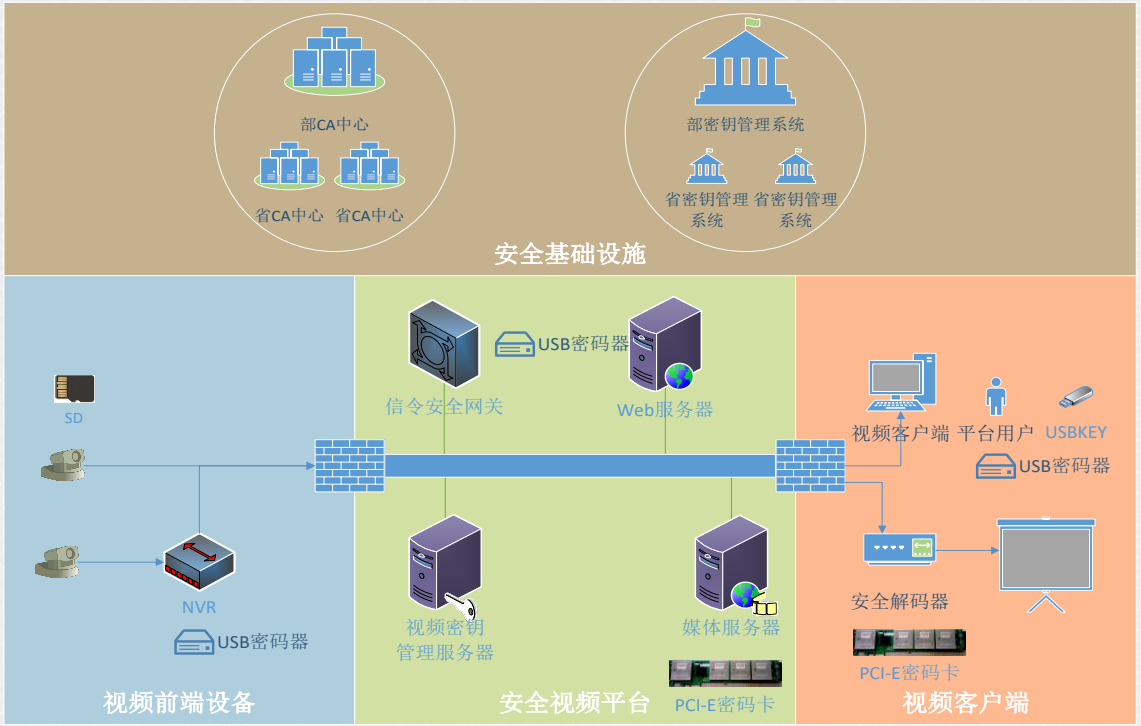
1. 2016年银监会发布了《中国银行业信息科技“十三五”发展规划监管指导意见》，指出银行业应该积极应用云计算、大数据等技术；
2. 基于云密码机构建了**密码资源池**、**加密服务平台**、**密钥管理系统**、**资源管控系统**等的典型密码服务功能；
3. 为金融应用提供**登录认证**、**交易安全**、**数据防篡改**、**数据加密**等功能。

应用系统密码技术应用案例——快递行业隐私数据加密

1. 国家加大对快递行业个人敏感信息泄露的管理；
2. 江南天安针对快递行业应用的特点，推出了一系列的加密解决方案，包括：**应用层加密**、**数据库透明加密**、**文件存储加密**等；
3. 实现“**面单加密**”。

应用系统密码技术应用案例——公安行业应用

1. 作为主要参与单位，参与编写《GB 35114-2017公共安全视频监控联网信息安全技术要求》，并于2018.11.1强制执行；
2. 采用国产密码算法保证视频设备、监控数据的安全；
3. 涉及智慧城市、雪亮工程、平安城市等项目领域。

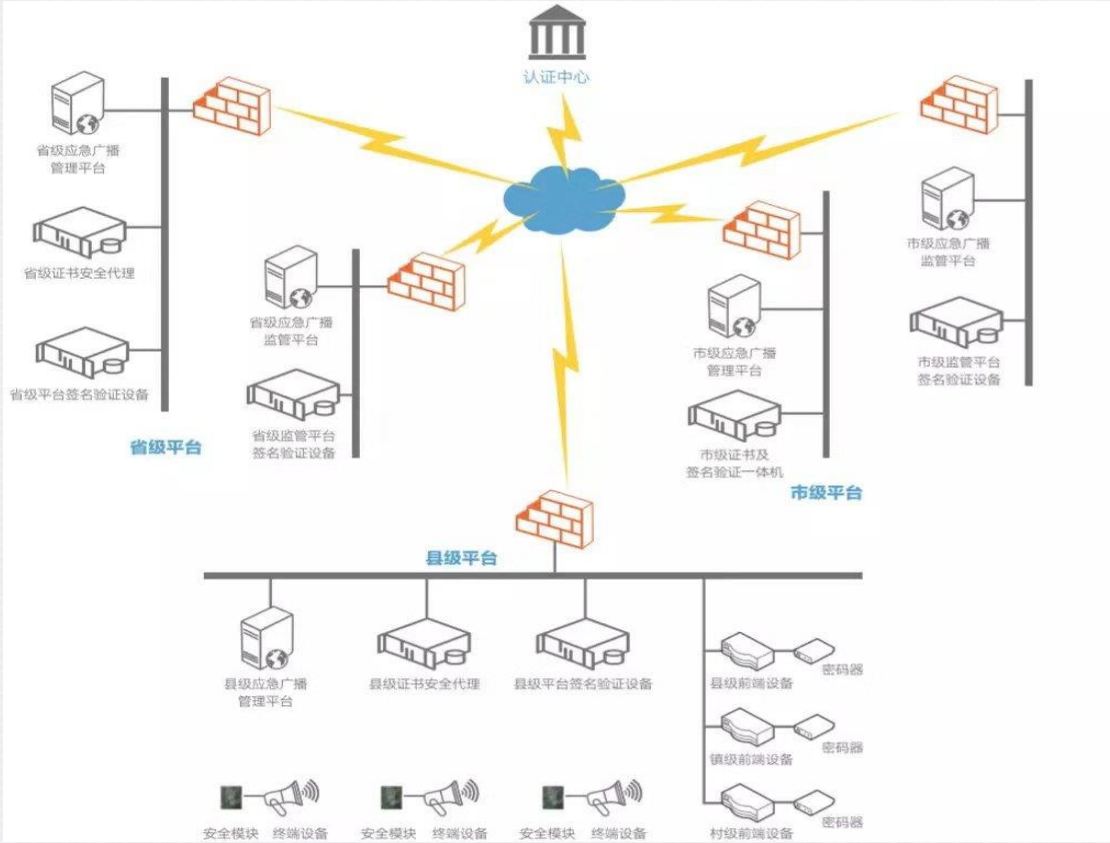


1. 建立了国家、省、市、县、乡、村等多级应急广播安全体系；

2. 基于**国产密码算法**；

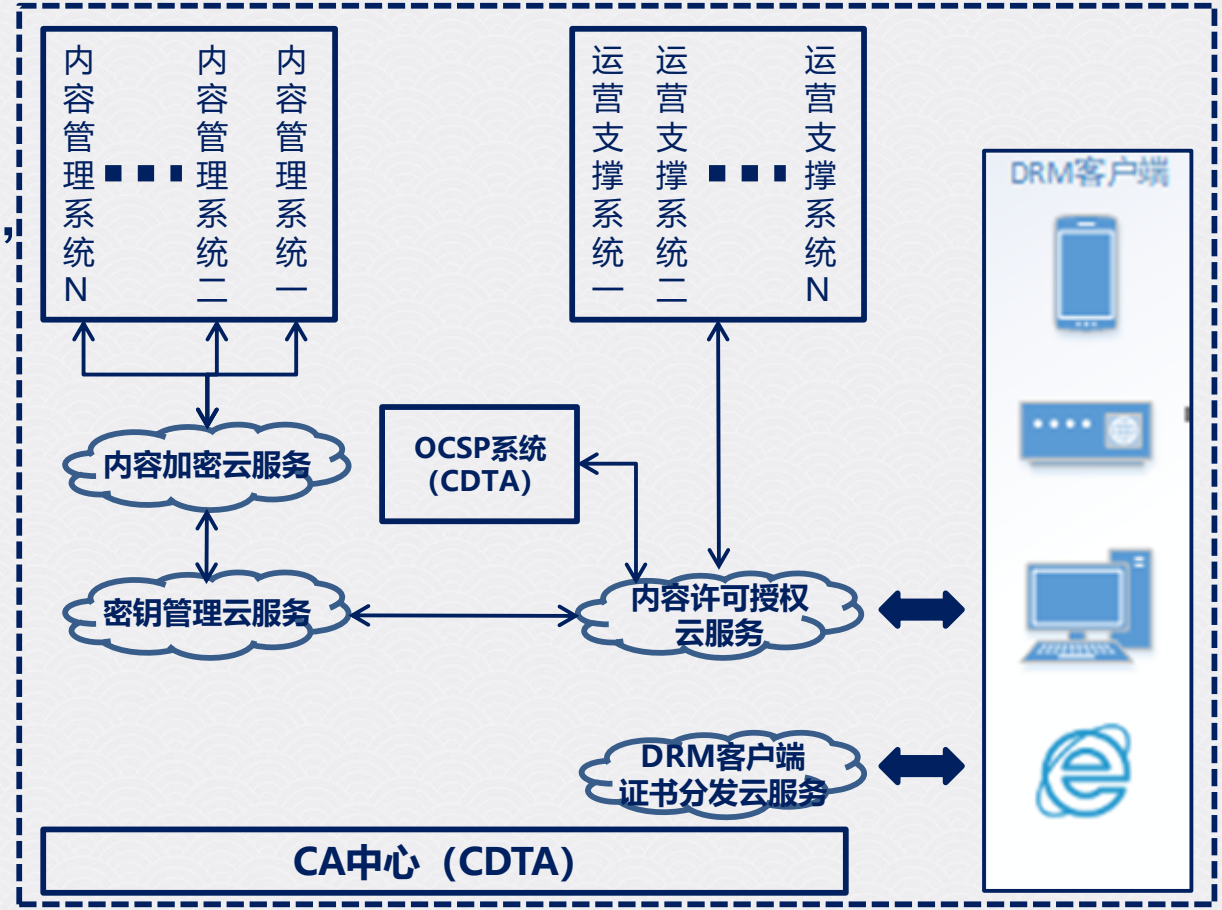
3. 保证应急广播指令和消息的**真实性**、**完整性**；

4. 实现整个应急广播系统的“**自主**、**安全**、**可控**”。



应用系统密码技术应用案例——广电行业DRM应用

1. ChinaDRM组织成员；
2. 参与DRM技术标准编写，标准中包含了国产密码算法要求。
3. 提供基于云环境的DRM内容许可授权服务、内容加密服务等。



CHINA'S LEADING CRYPTOGRAPHY TECHNOLOGY AND INFORMATION SECURITY COMPREHENSIVE SERVICES PROVIDER

中国领先的密码技术与信息安全综合服务商

谢谢各位领导和专家！

2019年1月18日