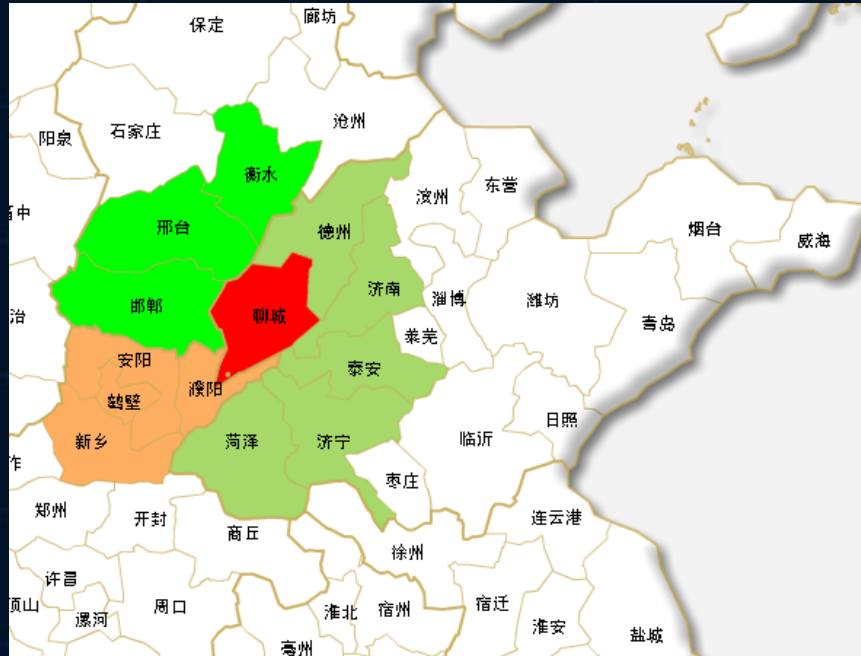




医院信息系统建设中商用密码应用探讨

聊城市人民医院 任立群

2021.4.23 杭州



- 在全省医院综合绩效考核中，医院连续四年排名全省第四；
- 香港艾力彼医院管理研究中心对大陆非省会城市三级综合医院排名，2017-2020我院连续4年全国第5名



医院概况



聊城市人民医院建于1947年，是一所集医疗、教学、科研、预防、保健于一体的三级甲等综合医院。山东省首批省级区域医疗中心，国家住院医师规范化培训基地及专科医师培训基地，国家临床药师培训基地，国家药物临床试验机构，国家干细胞临床研究机构，国家博士后科研工作站



医院概况



开放床位



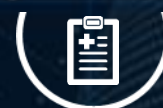
3200

临床医技科室



79

护理单元




120

2020年门急诊诊疗283.5万人次，出院病人12.6万人次，手术7.58万台次



人力资源



- 
- 现有职工5800余人，其中博士、硕士2662人，副高级职称以上人员1265人；
 - 博士、硕士研究生导师173人；
 - 国家级学术委员会副主任委员、常务委员、委员137人；
 - 省级学术委员会主任委员、副主任委员、常务委员239人；
 - 近年来，从美国、澳大利亚、荷兰、日本等国家引进外籍专家学者8名，全职从事科研与临床工作，柔性引进35名外籍专家。



人才培养



- 外聘中国工程院院士5人，外籍院士3人，引进国家“千人计划”专家2人，“泰山学者”特聘专家2人
- 先后选派500余名专业技术人员到国外进修、培训，攻读学位
- 鼓励并支持科室及130余名专业技术和实验室人员参与国际化的医学研究
- 分别与武汉大学和山东大学联合举办了4届博士研究生培训班，联合培养博士生156名





设备信息



配置影像设备、手术设备、肿瘤治疗设备、急救生命支持类设备、内镜设备、实验室设备等大型医疗、教学、科研设备1万余台件，设备总值14亿元。



256排revolution螺旋CT



PET-CT



3.0T静音磁共振



陀螺刀



全数字直线加速器



数字化平板血管机



复合手术室
(数字平板+内窥镜+腔镜 联合手术室)



飞秒激光治疗仪



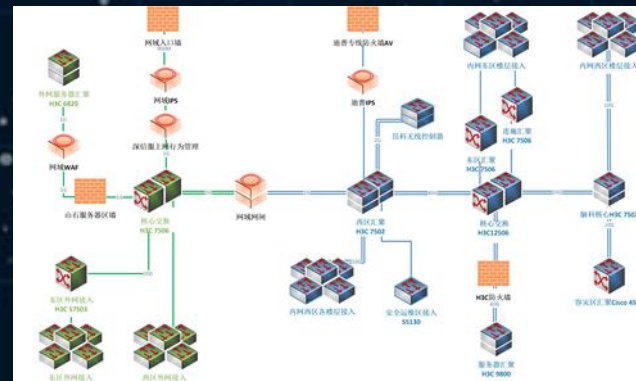
256排revolution螺旋CT

PET-CT



信息化建设

- 建立了以电子病历为核心的医院信息管理系统，涵盖医嘱、护理、影像、检验、病理、药学、麻醉、输血、急救、科研、健康管理等200余个子系统；
- 通过了网络安全等级保护三级、电子病历分级评价4级、互联互通成熟度评测4级甲等；
- 拥有一支自主开发能力较强的专业信息技术团队，年更新系统/应用模块110余项；
- 利用大数据、人工智能、物联网、5G等技术，全方位提高医疗质量、科研能力，提升患者就医体验，保障患者安全。逐步建成了以数据为驱动的智慧化数字医院。





- **01** | 密码的相关概念
- **02** | 医院信息系统商用密码使用分析
- **03** | 医院信息系统建设中商用密码应用



01

密码的相关概念

1.1

密码及其分类

1.2

密码的重要作用

1.3

密码应用领域政策要求



1.1 密码及其分类



密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。



口令 ≠ 密码



1.1 密码及其分类



对称算法 { ZUC、SM4、SM1（尚未公开发布）SM7（尚未公开发布）
国外算法：DES、TDES、AES

非对称（公钥）算法 { SM2、SM9
国外算法：RSA

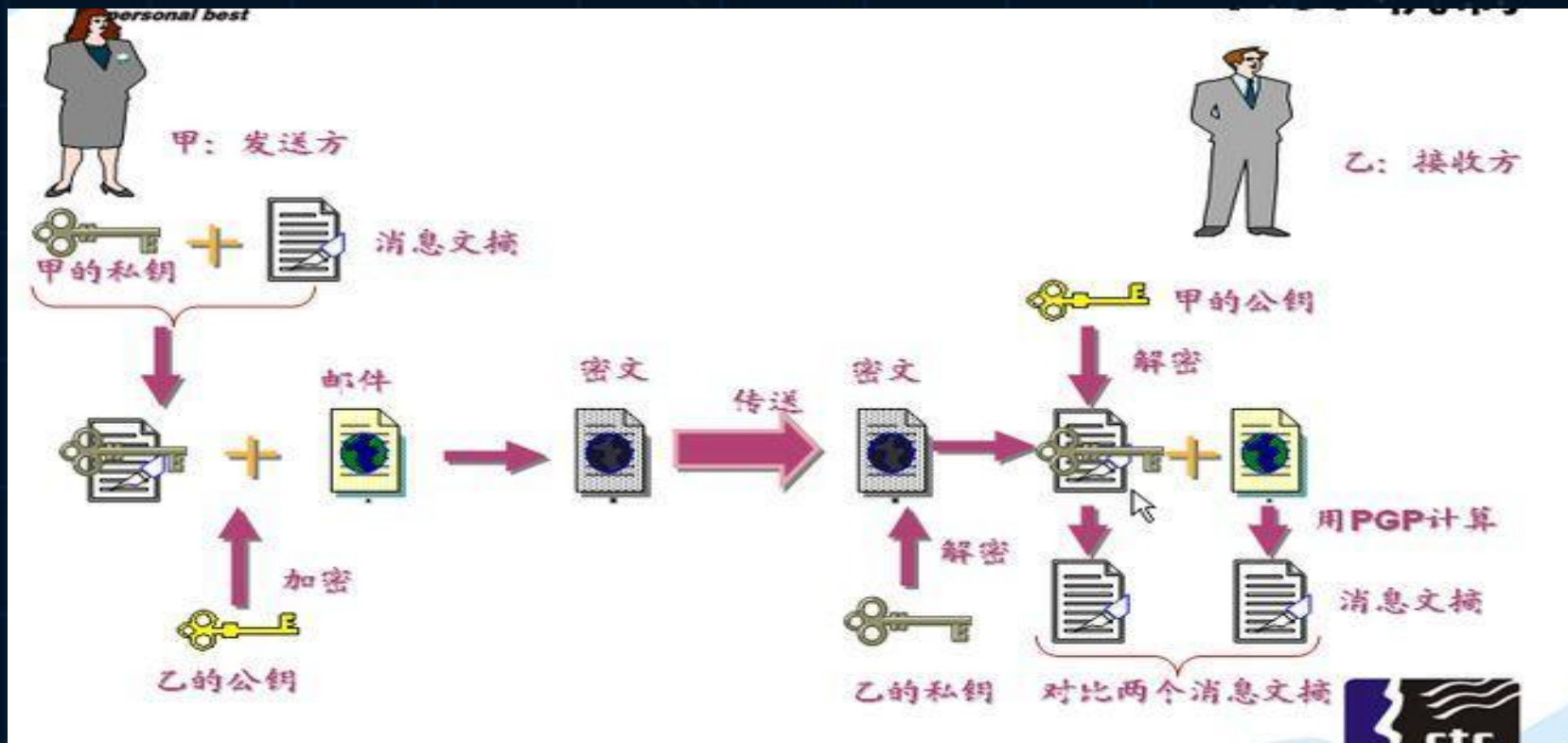
杂凑算法 { SM3
国外算法：MD5、SHA



1.1 密码及其分类



非对称（公钥）算法





1.2 密码重要作用



密码是保证网络与信息安全的核心技术和基础支撑

真实性	➡	防假冒	进不来
保密性	➡	防泄漏	看不懂
完整性	➡	防篡改	改不了
不可否认性	➡	防抵赖	跑不掉



1.2 密码重要作用



- 密码技术是实现网络从被动防御向主动防御转变的重要因素
- 密码技术是构建网络信任体系的基础
- 密码技术是保护国家社会稳定、促进经济发展的战略资源
- 密码技术是保护自身权益及个人隐私的关键手段



1.3 密码应用领域政策要求



1999年国务院颁布《商用密码管理条例》，对商用密码产品的科研、生产、销售和使用实施管理。

2002年国家商用密码办公室成立。

商用密码管理条例	
颁布单位：国务院	文号：第273号
颁布日期：1999-10-07	执行日期：1999-10-07
时 效 性：现行有效	效力级别：行政法规

目录
第一章 总则
第二章 科研、生产管理
第三章 销售管理
第四章 使用管理
第五章 安全、保密管理
第六章 罚则
第七章 附则



1.3 密码应用领域政策要求



2019年10月26日十三届全国人大常委会第十次会议通过，习近平主席签署第35号主席令正式颁布，自2020年1月1日起正式实施

- 密码领域综合性、基础性的法律
- 旨在规范密码使用和管理，促进密码事业发展，保证网络和信息安全，提升密码管理科学化、规范化、法治化水平





1.3 密码应用领域政策要求



第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。**商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接**，避免重复评估、测评。

第三十一条 密码管理部门和有关部门建立日常监管和随机抽查相结合的商用密码事中事后监管制度，建立统一的商用密码监督管理信息平台，**推进事中事后监管**与社会信用体系相衔接，强化商用密码从业单位自律和社会监督。

第三十七条 关键信息基础设施的运营者违反本法第二十七条第一款规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者违反本法第二十七条第二款规定，使用未经安全审查或者安全审查未通过的产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。





1.3 密码应用领域政策要求



《信息安全等级保护商用密码管理实施意见》

- 第三级及以上信息系统的商用密码应用系统建设方案应当通过密码管理部门组织的审评后方可实施。
- 各省(区、市) 第三级信息系统的商用密码应用系统建设方案，由信息系统的责任单位向所在省(区、市) 密码管理部门提出评审申请，所在省(区、市) 密码管理部门组织专家进行评审。
- 第三级以上信息系统的商用密码应用系统，应当通过国家密码管理部门指定测评机构的密码测评后方可投入运行。密码测评包括资料审查、系统分析、现场测评、综合评估等
- 本意见施行前已建成的第三级以上信息系统的商用密码应用系统，应当按照本意见第八条的要求进行密码测评，并根据密码测评意见实施改造。

《关键信息基础设施安全保护条例（征求意见稿）》

- 运营单位对保护工作部门开展的网络安全检查工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的检查应当予以配合。
- 关键信息基础设施密码的使用和管理，还应当遵守密码法律、行政法规的规定。



1.3 密码应用领域政策要求



等保2.0通用要求VS等保1.0（三级）有关“密码”技术要求对比

通信传输	a) 应采用校验码技术或密码技术保证通信过程中数据的完整性；
	b) 应采用密码技术保证通信过程中敏感信息字段或整个报文的保密性。
身份鉴别	d) 应采用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使用动态口令、密码技术或生物技术来实现。
数据完整性	a) 应采用校验码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个人信息等；
	b) 应采用校验码技术或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个人信息等。
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、重要业务数据和重要个人信息等；
	b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。



1.3 密码应用领域政策要求

GM/T 0054-2018 《信息系统密码应用基本要求》

- 在密码功能要求中，规定了信息系统中需要使用密码技术保护的對象，包括机密性、完整性、真实性、不可否认性。
- 在密码技术应用要求中，规定了密码技术的应用要求，要求项依据等级增加而增强，包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全。
- 在密钥管理中，对密钥的全生命周期提出了要求，包括密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁。
- 在安全管理中，规定了密码安全管理要求，包括制度、人员、实施、应急，其中实施分为规划、建设、运行。

GB/T 39786

- 2021年3月，国家市场监督管理总局、国家标准化管理委员会发布中华人民共和国国家标准公告（2021年第3号），国家密码应用与安全性评估的关键标准GB/T 39786—2021《信息安全技术信息系统密码应用基本要求》正式发布，将于2021年10月1日正式实施。
- GB/T 39786是贯彻落实《中华人民共和国密码法》、指导我国商用密码应用与安全性评估工作开展的纲领性、框架性标准。该标准分五个级别，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面提出了密码应用技术要求，从管理制度、人员管理、建设运行和应急处置四个方面提出了密码应用管理要求，对于规范引导信息系统密码合规、正确、有效应用具有重要意义。



1.3 密码应用领域政策要求



商用密码应用系统

密码安全能力支撑

密码安全服务支撑

密码管理基础设施	运维管理	密码应用层	安全电子邮件系统 可信时间戳系统		安全公文传输 权限管理系统 通用密码应用		桌面安全防护 电子印章系统		技术要求	密码模块	采用符合相关标准要求的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				
	信任管理	密码服务层	对称密码服务		公钥密码服务 密码应用程序接口		其它密码服务			应用与数据	数据传输 / 数据存储 / 访问控制信息 / 日志记录 / 身份鉴别 / 应用程序				
			安全芯片类		密码模块类		密码整机类			设备与计算	远程管理 / 访问控制信息 / 敏感标记 / 日志记录 / 身份鉴别 / 重要可执行程序				
			其它		其它		网络和通信	通信过程中的敏感字段或通信报文 / 集中管控 / 通信数据 / 网络边界访问控制信息 / 身份鉴别 / 安全准入认证							
	设备管理	密码支撑层	密码功能产品及其集成关系								物理和环境	电子门禁系统进出记录 / 视频监控音像记录 / 身份鉴别			
密钥管理	密码资源层	算法软件		算法IP核		算法芯片		其它		管理要求	管理制度	人员管理	密钥管理	密码生成	密码使用
		序列算法	分组算法	公钥算法	杂凑算法	随机数生成算法	其它	建设运行	应急处置		密码分发	密钥归档			
基础密码算法															



1.3 密码应用领域政策要求



医院信息互联互通标准化成熟度测评方案

4.3.3 数据安全	4.3.3.2	具有数据完整性（数据故障恢复）措施	0.2	四级乙等	满足要求得分 否则不得分	医院信息平台中涉及到医疗数据的传输、存储，可以采用电子签名及时间戳等相关技术来保证医疗数据的完整性以及可追溯性；可采用网络密码设备的加密、完整性验证、数据源验证、抗重播等技术实现信息在不可信网络上的安全传输。
	4.3.3.3	数据传输进行加密处理，关键数据可追溯	0.1	五级乙等	满足要求得分 否则不得分	
4.3.4 隐私保护	4.3.4.5	支持对关键个人病历信息（字段级、记录级、文件级）进行加密存储保护	0.3	五级甲等	满足要求得分 否则不得分	进行数据存储加密，加解密文件和其它数据块，用于保护在联机存储、备份或长期归档中的数据



1.3 密码应用领域政策要求



山东省卫生计生委文件

鲁卫函〔2017〕200号

山东省卫生计生委 关于开展全省卫生计生行业网络安全 现场检查工作的通知

11. 商用密码应用工作领导小组、商用密码相关规章和管理
制度、商用密码推进工作相关工作计划;



1.3 密码应用领域政策要求

山东省卫生计生行业网络安全工作评价指标(2017试行版V1.0)

4	网络安全专项管理	商用密码	商用密码应用	采重要网络系统（HIS、LIS、PACS、EMR、集成平台、临床数据中心）用国密算法对数据存储、传输及其应用进行保护	2	定量	$P = \text{采用国密算法防护信息安全的系统数量} / \text{重要网络系统总数}$
			可靠身份认证	对于医护（工作）人员采取数字证书等可靠机制建立起可信数字身份，利用数字身份认证机制，确保访问业务系统身份可信	2	定性	符合， $P = 1$ ；不符合， $P = 0$ 。
			电子签名签章	利用合法的第三方电子签名签章，保障电子病历、处方、公文等信息的真实性、完整性、机密性以及不可抵赖性	2	定性	符合， $P = 1$ ； 签名签章资质不全， $P = 0.3$ ； 不符合， $P = 0$ 。
			可信时间	配置部署统一时钟服务器，提供准确连续可靠时间服务	2	定性	符合， $P = 1$ ；不符合， $P = 0$ 。
			关键场景保护	采用技术措施，对于涉及医患双方签字等关键场景进行保护，可溯	2	定性	符合， $P = 1$ ；不符合， $P = 0$ 。
		等级保护	安全域划分	网络安全等级保护安全域（例如：网络域、用户域、计算域）划分合理	2	定性	符合， $P = 1$ ；不符合或者没开展等保工作， $P = 0$ 。
			等保备案	业务系统在公安部门备案	2	定量	$P = \text{备案系统总数} / \text{信息系统总数}$
			等保测评	开展等保测评工作	2	定量	$P = \text{已测评系统总数} / \text{信息系统总数}$
			等保测评机构	等保测评机构在国家等保协调小组办公室推荐名录，且与合同单位一致	2	定性	符合， $P = 1$ ；不符合或者没开展测评， $P = 0$ 。
			测评保密协议	与等保测评机构签订保密协议	2	定性	符合， $P = 1$ ；不符合或者没开展测评， $P = 0$ 。
			等保信息报送	等保定级信息向上级卫生计生委报送	2	定性	符合， $P = 1$ ；不符合或者没开展测评， $P = 0$ 。
		关键基础设施	信息资产配置排查工作	有单位信息资产清单或者台账	2	定性	符合， $P = 1$ ；不符合， $P = 0$ 。
			关键信息基础设施意识	了解关键信息基础设施政策情况	2	定性	符合， $P = 1$ ；不符合， $P = 0$ 。
			关键信息基础设施梳理工作	有关键信息基础设施清单（含无关键信息基础设施）	2	定性	符合， $P = 1$ ；不符合， $P = 0$ 。
		软件正版化	操作系统	服务器、PC所使用正版操作系统的情况	2	定量	$P = \text{正版数量} / \text{实际运行总数}$
			数据库系统	各业务系统使用正版数据库系统的情况	2	定量	$P = \text{正版数量} / \text{实际运行总数}$
			虚拟化系统	各种业务使用正版虚拟化软件的情况	2	定量	$P = \text{正版数量} / \text{实际运行总数}$
			办公软件	单位使用办公软件如 MSoffice 或者 WPSoffice 的情况	2	定量	$P = \text{正版数量} / \text{实际运行总数}$
			防病毒软件	单位使用正版防病毒软件的情况	2	定量	$P = \text{正版数量} / \text{实际运行总数}$



➤ 02 | 医院信息系统商用密码使用分析

2.1 | 医院信息系统特点

2.2 | 医院信息系统常见安全问题

2.3 | 医院信息系统商用密码现状及需求



2.1 医院信息系统特点



数据重要性

医院已逐渐向数据驱动型转变。数据成为质量提升、科研创新、闭环服务、绩效改革等诸多方向的基础

交互性强

互联互通、大数据环境下的必然，多类临床信息处理系统产生的数据被相互调用、流转、存储

数据种类多

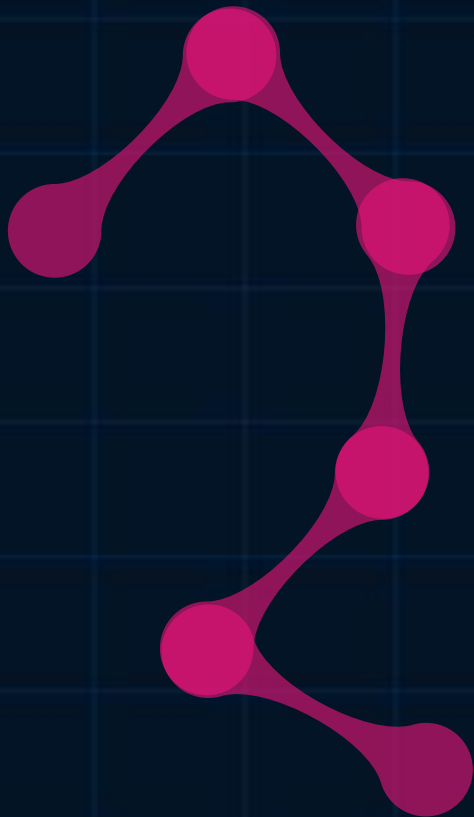
结构化与非结构化数据，应用中包括医疗终末静态数据，也包括医疗过程中的动态数据。

用户多样

提供医疗服务的医生护士医技人员、接受医疗服务的患者，以及参与医疗活动管理的人员



2.2 医院信息系统常见安全问题



医院运营数据及患者隐私数据被**不正当披露或泄露**、
影响社会安全、医院发展、个人安全

数据**超授权使用、不规范使用**，影响业务系统效率

数据被篡改，牵一发动全身，影响系统健壮性、业
务连续性 & 数据利用价值



2.3 医院信息系统商用密码应用现状及需求



1) 密码应用不广泛

- 大量敏感数据缺乏密码保护，处于裸奔状态
- 密码应用普遍缺乏系统性、整体性

2) 密码应用不规范

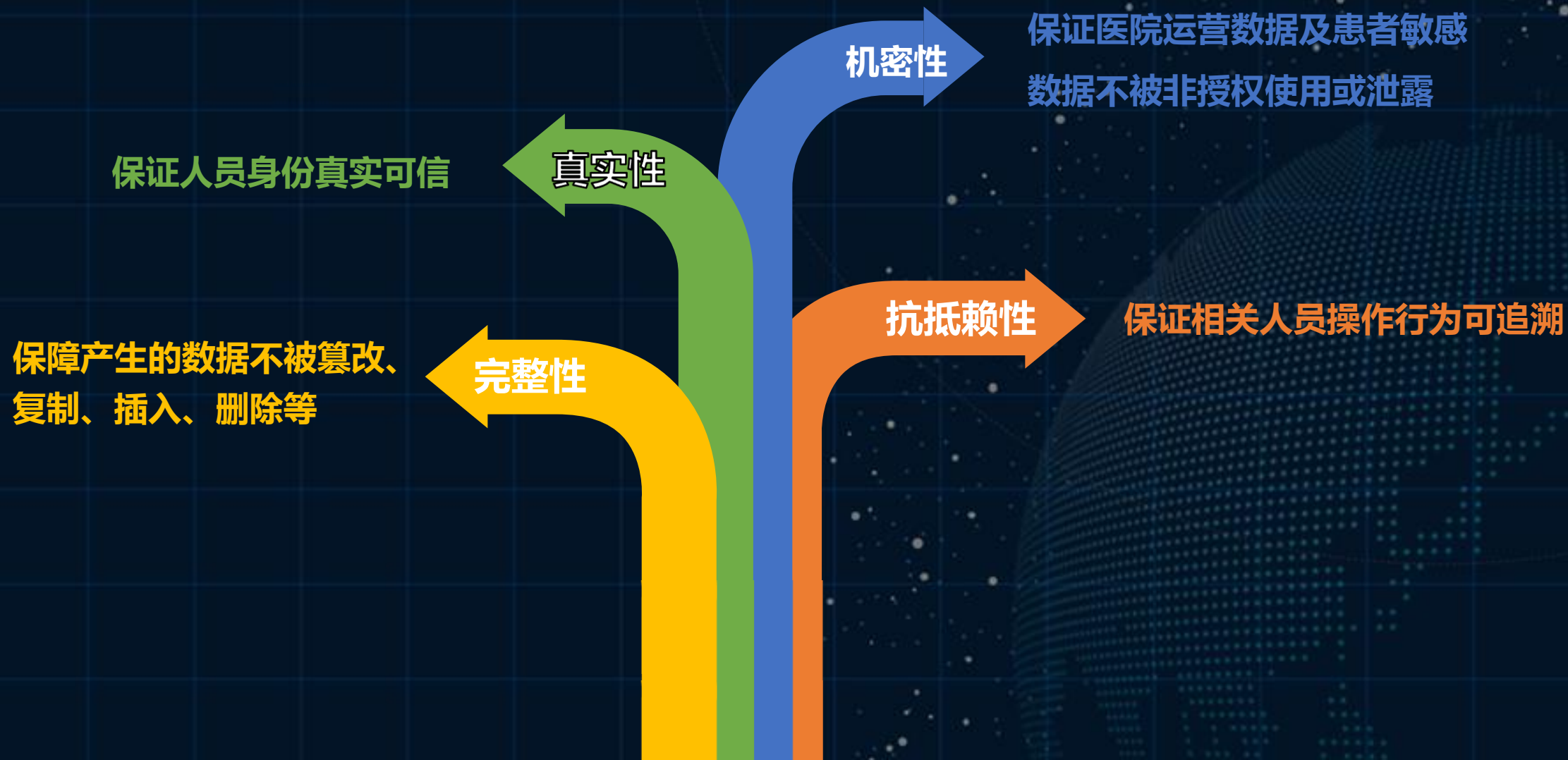
- 使用了基于国外的密码算法
- 使用了自行研制或者境外生产的密码产品
- 密码技术、密码产品未正确使用，密码保护措施无效

3) 密码应用不安全

- 大量系统使用了DES、MD5、SHA-1、RSA-1024等已被警示有风险的密码算法



2.3 医院信息系统商用密码应用现状及需求





03 | 医院信息系统建设中商用密码应用

- 3.1 | 信息系统生命周期中相关商用密码工作要求
- 3.2 | 落实GB/T39786-2021 要求
- 3.3 | 医院信息系统商用密码使用建议



3.1 信息系统生命周期中相关商用密码工作要求



系统
规划阶段

责任单位组织专家或委托密评机构对密码应用方案进行评估，评估通过后方可建设

系统
建设完成

系统责任单位委托密评机构开展密评，评估通过后方可投入运行

系统
运行阶段

定期开展密评，关键信息基础设施、三级及以上信息系统每年至少评估一次



3.1 信息系统生命周期中相关商用密码工作要求





3.1 信息系统生命周期中相关商用密码工作要求



- 系统现状分析
- 安全风险及控制需求
- 密码应用需求
- 总体方案设计
- 密码技术方案
- 管理体系和运维体系设计
- 安全与合规性分析

子系统、密码产品、密码服务、密码算法和协议、密码应用工作流程、密钥管理实现等

不适用项逐条论证，分析原因或寻找替代措施



3.1 信息系统生命周期中相关商用密码工作要求



密码应用应急处置方案

系统发生密码相关重大安全事件、重大调整或特殊紧急情况，应开展应急评估，依据评估结果进行应急处置

- 重点识别项目实施过程中可能发生的安全事件、密码设备运行过程中可能发生的安全事件
- 事件分类分级
- 应急处置组织结构与职责、技术和管理应急响应机制和风险防范措施
- 事件公告流程、损失评估程序、预案激活条件



3.1 信息系统生命周期中相关商用密码工作要求



什么是密评?

- 密评就是国家密码行政管理部门批准的测评机构根据标准要求，对不同测评单元给出测评结果，并判断密码应用实际情况是否解决相应安全问题的过程。

哪些系统需要做密评？

- 关键信息基础设施、等级保护第三级及以上信息系统

密评如何定级？

- 目前密评系统的定级参照等级保护的系统定级

密码评测



3.2 落实GB/T39786-2021 要求



参考国家标准GB/T39786—2021 《信息安全技术信息系统密码应用基本要求》
从以下四大方面落实商用密码应用**技术要求**





3.2 落实GB/T39786-2021 要求



物理和环境安全



物理和环境安全是信息系统安全最基础部分，需要利用密码技术有效地保护进入机房等重要场所的人员身份的真实性以及视频、进出记录数据的完整性

- 部署核准的电子门禁（保护物理访问控制身份鉴别信息）
- 采用MAC或数字签名等技术保护电子门禁进出记录和视频监控记录的完整性

序号	项目	参数	备注
1	密码算法	国密SM7/SM1 算法	国密局认可
2	支持IC卡	国密SM7算法 IC卡，国密SM1算法 CPU卡	国密局认可
3	兼容卡片	其他符合ISO14443A的卡片 如S50/S70 MifareDesFire 等	
4	通讯协议	ISO14443 Type A	
5	遵循标准	ISO14443，ISO7816，FCC，CE	
6	状态显示	LED灯指示电源和通讯状态	
7	外形尺寸	114*74*20	
8	电压电流	12V150mA	
9	外部接口标准	Wiegand26/34/36 用户选定	
10	接口电缆长度	不大于80M	
11	读卡次数	10万次以上	
12	温度范围	-20 至 +60	
13	读卡距离	5cm至 8cm	





3.2 落实GB/T39786-2021 要求

网络和通信安全

网络层需要实现以下密码功能：对通信双方的身份进行鉴别、对通信过程中的数据做完整性保护、通信过程中的敏感数据或整个报文做机密性保护、对网络边界访问控制信息或系统资源访问控制信息的完整性进行保护和建立一条安全信息传输通道对网络中的安全设备进行集中管理。

选项	IPSec VPN	SSL VPN
身份认证	单向身份认证 双向身份认证 数字证书	双向身份认证 数字证书
加密	强加密 基于 web	强加密 依靠执行
全程安全性	端到端安全 从客户到资源端全程加密	网络边缘到客户端 仅对客户到 VPN 网关之间通道加密
可访问性	选用与任何时间、任何地点访问	限制适用于已经定义好受控用户的访问
费用	低（无需任何附加客户端软件）	高（需要客户端软件）
安装	即插即用安装 无需任何附加的客户端软、硬件安装	通常需要长时间的配置 需要客户端软件或者硬件
用户的易用性	对用户非常友好，使用非常熟悉 web 浏览器 无需终端用户的培训	对没有相应技术的用户比较困难 需要培训
支持的应用	基于 web 的应用 文件共享 E-mail	所有基于 IP 协议的服务
用户	客户、合作伙伴用户、远程用户、供应商等	更适用于企业内部使用
可伸缩性	容易配置和扩展	在服务器端容易实现自由伸缩，在客户端比较困难



- 网络边界部署核准的IPSec VPN或SSL VPN



3.2 落实GB/T39786-2021 要求



设备和计算安全



设备和计算层面主要利用密码技术保证终端设备、服务器、安全设备和操作系统等算法运行及计算环境安全。计算与设备层需要实现以下密码功能：对系统中登录设备的用户进行身份鉴别、对系统日志、访问控制信息、重要程序或文件、重要信息资源敏感标记进行完整性保护以及远程管理时身份鉴别信息需做机密性保护

- 采用数字证书登录、OTP等进行设备登录（身份鉴别）
- 调用密码机实现重要数据的完整性保护





3.2 落实GB/T39786-2021 要求



应用和数据安全



应用与数据层需要实现以下密码功能：对登录的用户进行身份鉴别、保证系统资源访问控制信息和重要资源信息敏感标记和日志的完整性、对传输和存储过程中数据的机密性和完整性进行保护、重要程序的安装及卸载进行安全控制

- 重要业务数据
- 重要用户数据
- 重要配置数据
- 重要审计数据



3.2 落实GB/T39786-2021 要求



应用和数据安全



应用与数据层需要实现以下密码功能：对登录的用户进行身份鉴别、保证系统资源访问控制信息和重要资源信息敏感标记和日志的完整性、对传输和存储过程中数据的机密性和完整性进行保护、重要程序的安装及卸载进行安全控制

以一个CS结构的服务为例：

- 客户端本地数据存储
- 客户端和服务端的通信
- 服务端各种配置文件
- 服务端相关的存储中间件交互保存数据
- 不同的客户端（其他系统）需要传输和分享的数据



3.2 落实GB/T39786-2021 要求

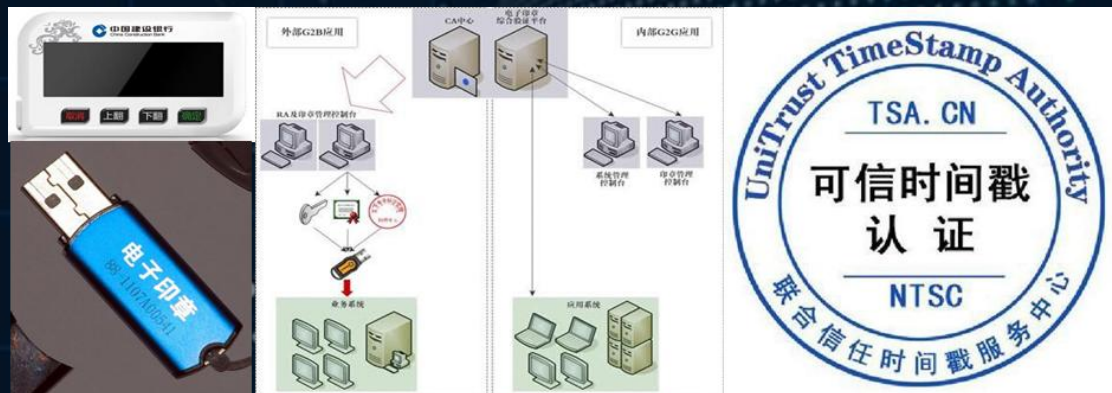


应用和数据安全



应用与数据层需要实现以下密码功能：对登录的用户进行身份鉴别、保证系统资源访问控制信息和重要资源信息敏感标记和日志的完整性、对传输和存储过程中数据的机密性和完整性进行保护、重要程序的安装及卸载进行安全控制

- 采用智能密码钥匙、动态令牌登录应用系统（身份鉴别）
- 部署密码机对数据加密后传输、存储（机密性保护）
- 应用系统部署电子签章、时间戳服务器（抗抵赖）





3.2 落实GB/T39786-2021 要求



制度

- 制定密码安全管理制度及操作规范
- 定期论证和审定
- 明确相关管理制度发布流程
- 制度执行过程应留存相关记录

实施

- 规划阶段制定密码应用方案
- 实施阶段制定实施方案
- 评估通过后方可正式运行
- 每年委托密评机构开展评估
- 应急评估

应急

- 制定应急预案，做好应急资源准备
- 事件发生后，及时上报
- 事件处置完成后，及时上报

人员

- 了解并遵守密码相关法律法规
- 能够正确使用密码产品
- 设置密钥管理员、安全审计员、密码操作员等关键岗位，建立岗位责任制度
- 建立人员培训、考核、保密、调离制度



3.3 医院信息系统商用密码使用建议



- 系统建设前同步规划、同步建设、同步进行网络安全保护、保密和密码保护措施
- 商用密码应用系统建设方案应当通过相关部门组织的评审
- 商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评（与等保相结合）
- 目前已上线的业务系统，多采用加密机、数据库加密机等设备实现，改造时要经过充分的论证与测试，避免对系统效率造成较大负面影响
- 如果刚接触商密并不熟，可委托第三方进行方案设计，方案完成后需经过专家论证或者测评机构评审。方案应包含密码应用设计方案、实施方案和应急方案三部分。



3.1 信息系统生命周期中相关商用密码工作要求



方案设计原则

总体品性优势原则

- 密码应用与信息系统的业务相结合才能发挥密码的作用
- 遵循顶层设计原则，明确应用需求，通过总体方案和密码支撑体系总体架构设计，引导密码在信息系统中的应用

科学性原则

- 成体系、分层次设计，避免照搬标准、堆砌密码设备
- 避免重复建设和过度保护

完备性原则

- 从物理和环境、网络和通信、设备和计算、应用和数据、密钥管理、安全管理等方面，建立完备的密码支撑保障体系

可行性原则

- 保证信息系统业务的正常运行，兼顾部分信息系统的复杂性和兼容性
- 通过评审的密码应用方案可采取分步实施、稳步推进的策略



| 小结



倡导“三个新”

- 第一个是新安全文明：即通过密码实现可信互联、安全互通，倡导网络空间开放、共享、安全的发展理念；
- 第二个是新安全体制：即树立以总体国家安全观为统领，以密码为核心技术和基础支撑的网络信息安全观；
- 第三个是新安全环境：即构建以密码基础设施为底层支撑的，系统的、完善的网络安全保障体系。



感谢您的倾听
不当之处请批评指正