人脸识别应用产品及相关数据传输技术要求宣贯

上 海 安 全 防 范 报 警 协 会

www.sh-anfang.org

《人脸识别应用产品及相关数据传输技术要求》宣贯

条文解读

- 一 发布背景
- 二 条文大纲
- 三 术语解释
- 四 适用行业

技术要点

- 五 技术要求
- 六 传输要求
- 七 评审要点
- 八 验收要点

一 发布背景

上海市公安局技术防范办公室

沪公技防〔2021〕5号　　签发人：单雪伟

关于印发《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）》的通知

各公安分局、市局有关单位技术防范办公室，各技防产品、工程检测机构，各技防从业单位，各技防专家：

根据《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》（法释〔2021〕15号）中对使用人脸识别技术处理个人信息的相关要求，为进一步规范本市安防工程中人脸识别技术的应用，确保公民权益不被侵害，我办组织相关企业、检测机构、专家等对《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）》（见附件，以下简称“《技术要求》”）进行了多次讨论研究。现将《技术要求》印发给你们，请遵照执行。

自2022年3月1日起，本市安全技术防范工程评审方案（以下简称“方案”）系统中使用带人脸识别技术的安防产品，除符合现行标准规范要求外，还应符合本《技术要求》要求（如相关要求有冲突，以本《技术要求》为准），原产品系统中不符合要求的安防产品不得在方案中继续使用。

1

特此通知。

附件：《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）》

上海市公安局技术防范办公室

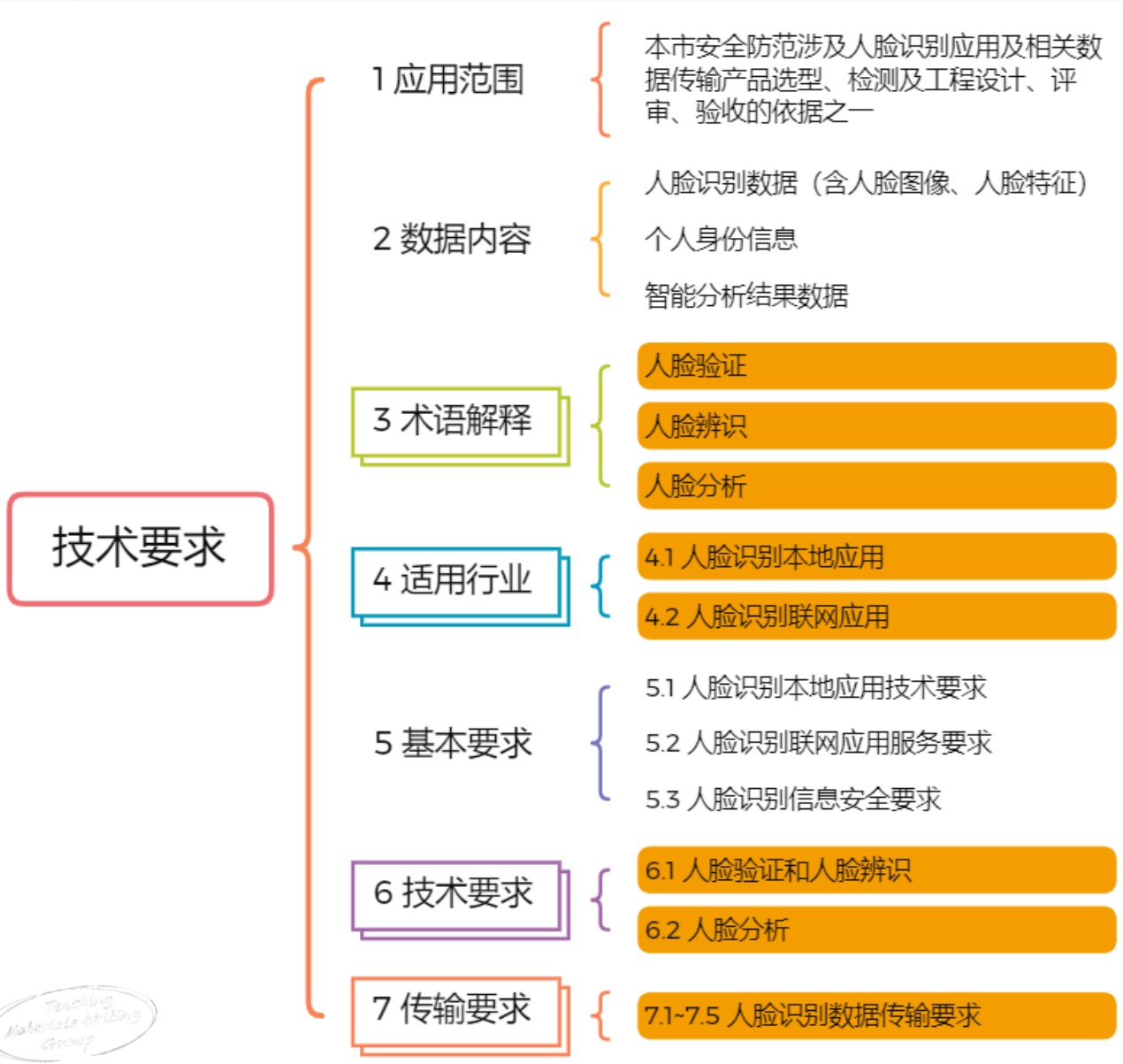
2021年12月13日

2022年3月1日
与涉及人脸识别
相关标准
并行实施

上海市公安局技术防范办公室　　2021年12月13日印发

2

二 条文大纲



应用范围

- ✓ 涉及人脸识别应用及相关数据传输
- ✓ 产品选型、检测
- ✓ 工程设计、评审、验收

数据内容

- ✓ 人脸识别数据（人脸图像、人脸特征）
- ✓ 个人身份信息
- ✓ 与人脸相关的智能分析结果

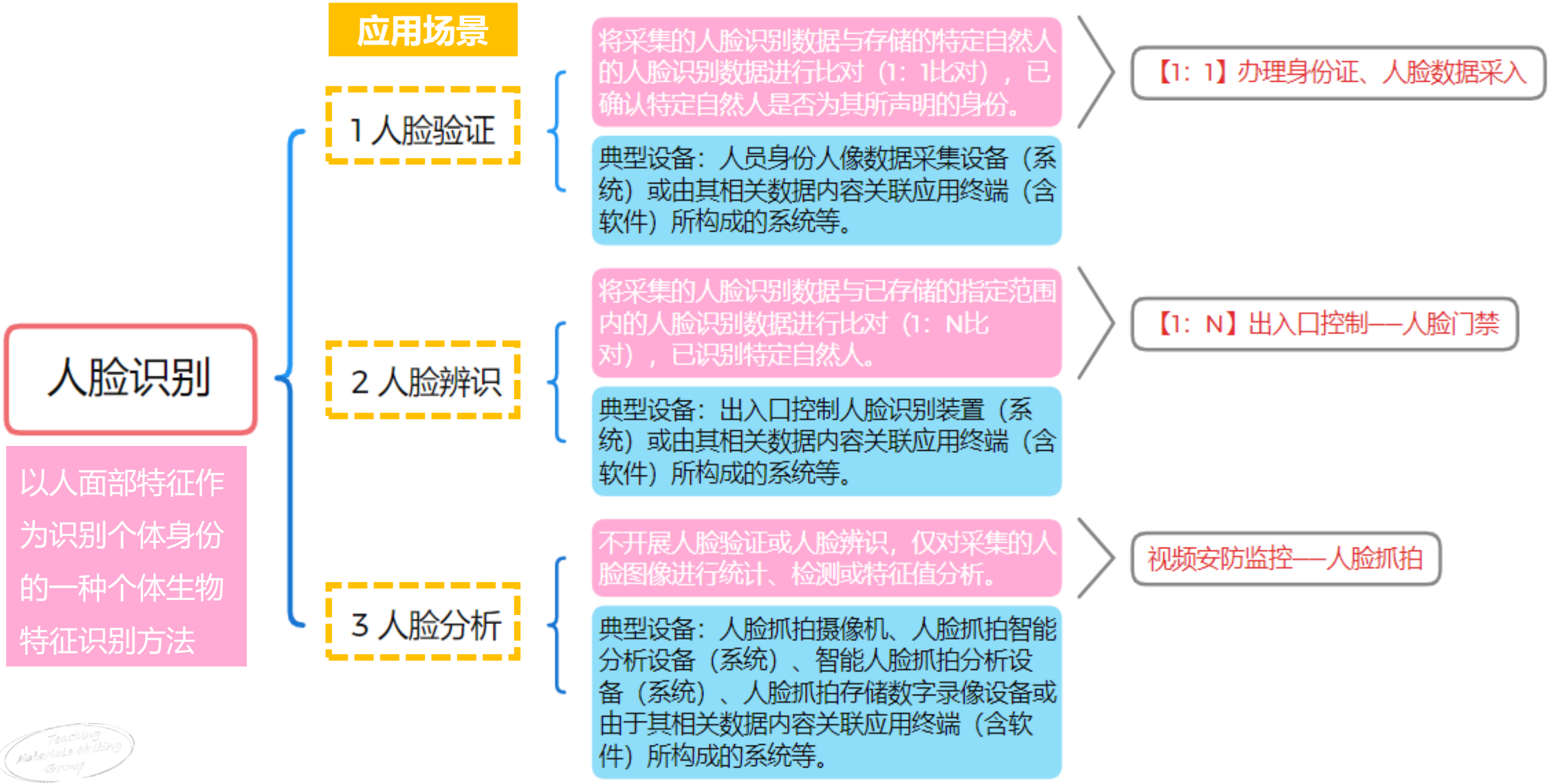
二 条文大纲—相关标准

- √ GB/T 20271 信息安全技术 信息系统通用安全技术要求
- √ GB/T 31488 安全防范 视频监控人脸识别系统技术要求
- √ GB/T 35273 信息安全技术 个人信息安全规范
- GB 37300 公共安全重点区域视频图像信息采集规范
- √ GB/T 38671 信息安全技术远程人脸识别系统技术要求
- GB 50348 安全防范工程设计规范
- √ 信息安全技术 生物特征识别信息保护基本要求
- √ 信息安全技术 网络数据处理安全规范

- √ GA/T 922.2 安防人脸识别应用系统 第2部分：人脸图像数据
- √ GA/T 1093 出入口人脸识别系统技术要求
- √ GA/T 1325 安全防范 人脸识别应用视频图像采集规范
- √ GA/T 1344 安防人脸识别应用 视频人脸图像提取技术要求
- √ GA/T 1755 安全防范人脸识别应用认证验证设备通用技术要求

- **DB31/T 294 住宅小区智能安全技术防范系统要求**
- DB31/T 329.1 第1部分：展览馆、博物馆
- DB31/T 329.2 第2部分：剧毒化学品、放射性同位素集中存放场所
- DB31/T 329.3 第3部分：金融机构
- DB31/T 329.4 第4部分：公共供水
- DB31/T 329.5 第5部分：电力设施
- DB31/T 329.6 第6部分：中小学、幼儿园、托育机构
- DB31/T 329.7 第7部分：城市轨道交通
- DB31/T 329.8 第8部分：旅馆、商务办公楼
- DB31/T 329.9 第9部分：零售商业
- DB31/T 329.10 第10部分：党政机关
- DB31/T 329.11 第11部分：医疗机构
- DB31/T 329.12 第12部分：通信单位
- DB31/T 329.13 第13部分：枪支弹药生产、经销、存放、射击场所
- DB31/T 329.14 第14部分：燃气系统
- DB31/T 329.15 第15部分：公交车站及公交专用停车场(库)
- DB31/T 329.16 第16部分：港口、码头
- DB31/T 329.17 第17部分：监管场所
- DB31/T 329.18 第18部分：渡轮、浏览船
- DB31/T 329.19 第19部分：寄递单位
- DB31/T 329.21 第21部分：养老机构
- DB31/T 329.22 第22部分：军工单位
- DB31/T 329.23 第23部分：大型活动场所
- DB31/T 329.24 第24部分：高校
- DB31/T 512 航空货运代理企业仓储场所
- **DB31/T 1099 单位（楼宇）智能安全技术防范系统要求**

三 术语解释


人脸识别
以人面部特征作为识别个体身份的一种个体生物特征识别方法
应用场景
1 人脸验证
将采集的人脸识别数据与存储的特定自然人的人脸识别数据进行比对（1：1比对），已确认特定自然人是否为其所声明的身份。
典型设备：人员身份人像数据采集设备（系统）或由其相关数据内容关联应用终端（含软件）所构成的系统等。
【1：1】办理身份证、人脸数据采入
2 人脸辨识
将采集的人脸识别数据与已存储的指定范围内的人脸识别数据进行比对（1：N比对），已识别特定自然人。
典型设备：出入口控制人脸识别装置（系统）或由其相关数据内容关联应用终端（含软件）所构成的系统等。
【1：N】出入口控制——人脸门禁
3 人脸分析
不开展人脸验证或人脸辨识，仅对采集的人脸图像进行统计、检测或特征值分析。
典型设备：人脸抓拍摄像机、人脸抓拍智能分析设备（系统）、智能人脸抓拍分析设备（系统）、人脸抓拍存储数字录像设备或由于其相关数据内容关联应用终端（含软件）所构成的系统等。
视频安防监控——人脸抓拍

三 术语解释

信息系统安全

- ✓ 信息系统业务组成包括操作系统、数据库管理系统、业务应用系统、网络系统和独立的网络产品等。
- ✓ 信息系统安全保护包括信息系统的安全运行控制和对运行中的信息系统所存储、传输和处理的信息的安全保护。
- ✓ 信息系统安全功能包括信息系统的物理安全、运行安全、数据安全三个方面。
- ✓ 信息系统安全等级包括所选用所需要的安全保护等级的安全产品，并按木桶原理进行综合分析、确定。

个人敏感信息

- ✓ 一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。
- ✓ 包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14周岁以下（含）儿童的个人信息等。

生物特征加密

- ✓ 存储和传输的生物特征识别数据的保密性可以通过访问控制和各种形式的加密技术获得，如使用SM2或SM4加密算法。

★★ 传输重要数据和个人敏感信息，应采用加密等安全措施 ★★

四 适用行业

最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定

发布时间：2021-07-28 15:16:29

法释〔2021〕15号

（2021年6月8日最高人民法院审判委员会第1841次会议通过，自2021年8月1日起施行）

为正确审理使用人脸识别技术处理个人信息相关民事案件，保护当事人合法权益，促进数字经济健康发展，根据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国消费者权益保护法》《中华人民共和国电子商务法》《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，制定本规定。

第五条　有下列情形之一，信息处理者主张其不承担民事责任的，人民法院依法予以支持：

（一）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需而处理人脸信息的；

（二）为维护公共安全，依据国家有关规定在公共场所使用人脸识别技术的；

（三）为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理人脸信息的；

（四）在自然人或者其监护人同意的范围内合理处理人脸信息的；

（五）符合法律、行政法规规定的其他情形。

适用行业

✓ 住宅小区	DB31/T 294
✓ 重点单位重要部位	DB31/T 329.X
✓ 航空货运代理	DB31/T 512
➢ 公共安全	GB 37300

无相关标准支持不应配置及安装

无职能部门要求不应配置及接入

四 适用行业

GB 37300-2018《公共安全重点区域视频图像信息采集规范》

	重点公共区域采集部位
1	具有政治历史意义、经常性举办重大群众性集会、商业服务、文化宣传、宗教活动的主要区域、周边重要路段、路口
2	城市、乡镇主要路段、路口、立交桥、城市地下人行通道、隧道、过街天桥等主要通行区域
3	高速公路、国道、省市县际、城镇道路主要出入口、卡口、公安检查站、收费站通道、高速公路服务区
4	大型桥梁、隧道主要通行区域
5	城镇商业金融聚集区主要出入口、周边主要路段、路口
6	民用机场、铁路车站、港口、码头、长途汽车站等场所外的露天广场主要区域、重要通道、周边路段、路口
7	城市轨道交通车站周边路段、路口
8	其他重点公共区域

四 适用行业

GB 37300-2018《公共安全重点区域视频图像信息采集规范》

	重点行业、领域	涉及公共区域的采集部位
1	党政机关	单位主出入口及采集的图像能够覆盖到单位外围一定范围的部位
2	民用机场、铁路车站、港口、码头、城市轨道交通车站及列车、长途汽车站、城市公共汽电车站、加油（气）站等	民用机场航站楼安检区以外开放区域和航站楼周边区域的人员聚集部位；铁路车站、港口的出入口、售票大厅、候车大厅等开放区域的人员聚集部位；城市轨道交通列车及车站出入口、车站通达、安检区、车站站厅、站台等开放区域；长途汽车站的出入口、售票大厅、候车大厅等开放区域的人员聚集部位；城市公共汽电车站区及周边一定范围；加油（气）站车辆出入口、服务区
3	银行营业场所等金融机构	营业网点、自助网点主出入口及其外部一定区域，运钞交接区、营业大厅
4	寄递单位、物流园区等	寄递单位营业场所主出入口、营业大厅交寄接收区，物流园区主出入口
5	电力、电信、广电、油气、水利等行业	重点单位周边一定区域、重点线路沿线
6	大型商贸中心和大型农贸市场等	单位主出入口、营业场所人员聚集部位、运钞交接区及押运通道
7	学校、幼儿园等教育单位	单位主出入口及外部一定区域
8	医院	医院主出入口、挂号大厅、候诊大厅等开放区域的人员聚集部位及采集的图像能够覆盖到单位外一定范围的部位
9	歌舞娱乐厅、电子游戏厅、互联网上网服务营业场所等场所	场所出入口及采集的图像能够覆盖到场所外围的一定范围的部位
10	旅馆业、洗浴中心	宾馆、酒店等旅馆业营业场所及洗浴中心的主出入口、大厅、前台及采集的图像能够覆盖到外围一定范围的部位
11	展览馆、大型文化、体育场所和其他大型群众性活动举办场所等	活动场所的出入口、安检区、室外人员聚集区域（部位）
12	旅游景区	旅游景区主出入口、人员聚集区域（部位）
13	其他治安保卫重点单位	单位出入口及采集的图像能够覆盖到单位外围一定范围的部位

五 技术要求

基本技术要求

- ✓ 身份鉴别：应启用口令复杂度、连续登录失败锁定等技术措施；
- ✓ 访问控制：应对接入系统的设备进行验证，并可拒绝或允许其连接；
- ✓ 安全审计：应启用对重要用户行为、重要安全事件的审计措施，审计记录完整无缺失，审计数据满足有关法律法规的存储要求。

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.1 人脸验证和人脸辨识

6.1.1 人脸验证和人脸辨识收集人脸识别数据时，应向被收集者告知收集规则，包括但不限于收集目的、数据类型和数量、处理方式、存储时间等，并征得被收集明示同意。

6.1.2 人脸验证和人脸辨识应仅收集用于生成人脸特征所需的最小数量、最少图像类型的人脸图像，人脸验证应在完成验证后立即删除证件原始图像，人脸辨识在完成辨识后应立即删除人脸图像。

关注点 1

人脸验证和人脸辨识

人脸识别数据的收集规则

- 告知方法
- 告知内容
- 明示同意

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.1 人脸验证和人脸辨识

6.1.1 人脸验证和人脸辨识收集人脸识别数据时，应向被收集者告知收集规则，包括但不限于收集目的、数据类型和数量、处理方式、存储时间等，并征得被收集明示同意。

6.1.2 人脸验证和人脸辨识应仅收集用于生成人脸特征所需的最小数量、最少图像类型的人脸图像，人脸验证应在完成验证后立即删除证件原始图像，人脸辨识在完成辨识后应立即删除人脸图像。

关注点 2

人脸验证和人脸辨识

人脸识别数据的应用规则

- 最小数量最少图像类型
- 完成验证删除原始图像
- 完成辨识删除人脸图像

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.1.3 人脸验证和人脸辨识应生成可更新、不可逆、不可链接的人脸特征：

a）可更新：从同一人脸图像可产生不同的人脸特征，当特定人脸特征泄露时，可重新生成不同的人脸特征；

b）不可逆：无法从人脸特征恢复人脸图像；

c）不可链接：根据同一人脸图像产生的不同人脸特征之间不具备关联性。

关注点 3

人脸验证和人脸辨识

人脸特征数据的应用规则

- 可更新
- 不可逆
- 不可链接

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.1.4 人脸验证和人脸辨识应具备包括使用人脸照片、纸质面具、人脸视频、人脸合成动画等防假体攻击能力。

6.1.5 人脸验证和人脸辨识应采用物理隔离或逻辑隔离方式分别存储人脸识别数据和个人身份信息，数据使用期限到期应自动删除人脸识别数据或进行匿名化处理。

关注点 4

- 人脸验证和人脸辨识活体检测
  - ✓ 人脸照片、纸质面具
  - ✓ 人脸视频、合成动画
- 物理隔离或逻辑隔离存储解释
- 数据使用期限到期的处理方式

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.2 人脸分析

6.2.1 人脸分析不应开展人脸验证或人脸辨识应用，如需结合人脸验证和人脸辨识的人脸特征数据、个人身份信息实现智能分析应用的，建设单位或使用单位在采用人脸验证和人脸辨识收集人脸识别数据时，应向被收集者告知收集规则，包括但不限于收集目的、数据类型和数量、处理方式、存储时间等，并征得被收集者明示同意。

关注点 5

人脸分析的应用规则

- 不应将视频监控视频图像或视频监控人脸抓拍图像应用于人脸验证或人脸辨识。
- 如需实现智能分析应用的，应告知收集规则并征得被收集者明示同意。

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.2.2 人脸分析应仅收集用于生成人脸特征所需的最小数量、最少图像类型的人脸图像，应具有连续去重和间断去重处理功能。

a）连续去重的最小时间单位为秒。在连续抓拍过程中，抓拍去重后输出人脸图像应包括首尾人脸或最优人脸等。

b）间断去重的最小时间单位为分。在非连续抓拍过程中，抓拍去重后输出人脸图像应包括首尾人脸或最优人脸等。

关注点 6

人脸分析的去重要求

（最小数量、最少图像要求）

- 连续去重
- 间断去重

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.2.3 人脸分析通过统计、检测或特征的智能分析应实现禁行闯入、异常滞留、异常徘徊、出现异常等预警提示应用。

6.2.4 人脸分析应采用物理隔离或逻辑隔离方式分别存储人脸图像和人脸特征。数据使用期限到期应自动删除人脸识别数据。

关注点 7

人脸分析的应用要求

- 智能应用是安装人脸分析设备的必要条件

✓ 禁行闯入

✓ 异常滞留

✓ 异常徘徊

✓ 出现异常

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

6 人脸识别应用技术要求

6.2.3 人脸分析通过统计、检测或特征的智能分析应实现禁行闯入、异常滞留、异常徘徊、出现异常等预警提示应用。

6.2.4 人脸分析应采用物理隔离或逻辑隔离方式分别存储人脸图像和人脸特征。数据使用期限到期应自动删除人脸识别数据。

关注点 8

- 物理隔离或逻辑隔离存储解释
- 数据使用期限到期的处理方式

六 传输要求

数据传输要求

- 应采用满足数据传输安全策略相应的安全控制措施，如数据加密等，对人脸识别数据的传输进行保护，**应至少采用**SSL等方式加密传输人脸数据。

✓ 本《技术要求》“数据传输”特指离开物理安全环境的数据传输内容。

✓ 本《技术要求》“传输内容”特指人脸识别相关的数据，包括人脸图像、人脸特征、个人身份信息等。

★★ “应至少采用”即非唯一方法 ★★

★★ 可采用SSL加密传输 ★★

★★ 也可以采用智能数据加密传输设备、网络安全终端设备等进行加密传输 ★★

六 传输要求

常用密码简介

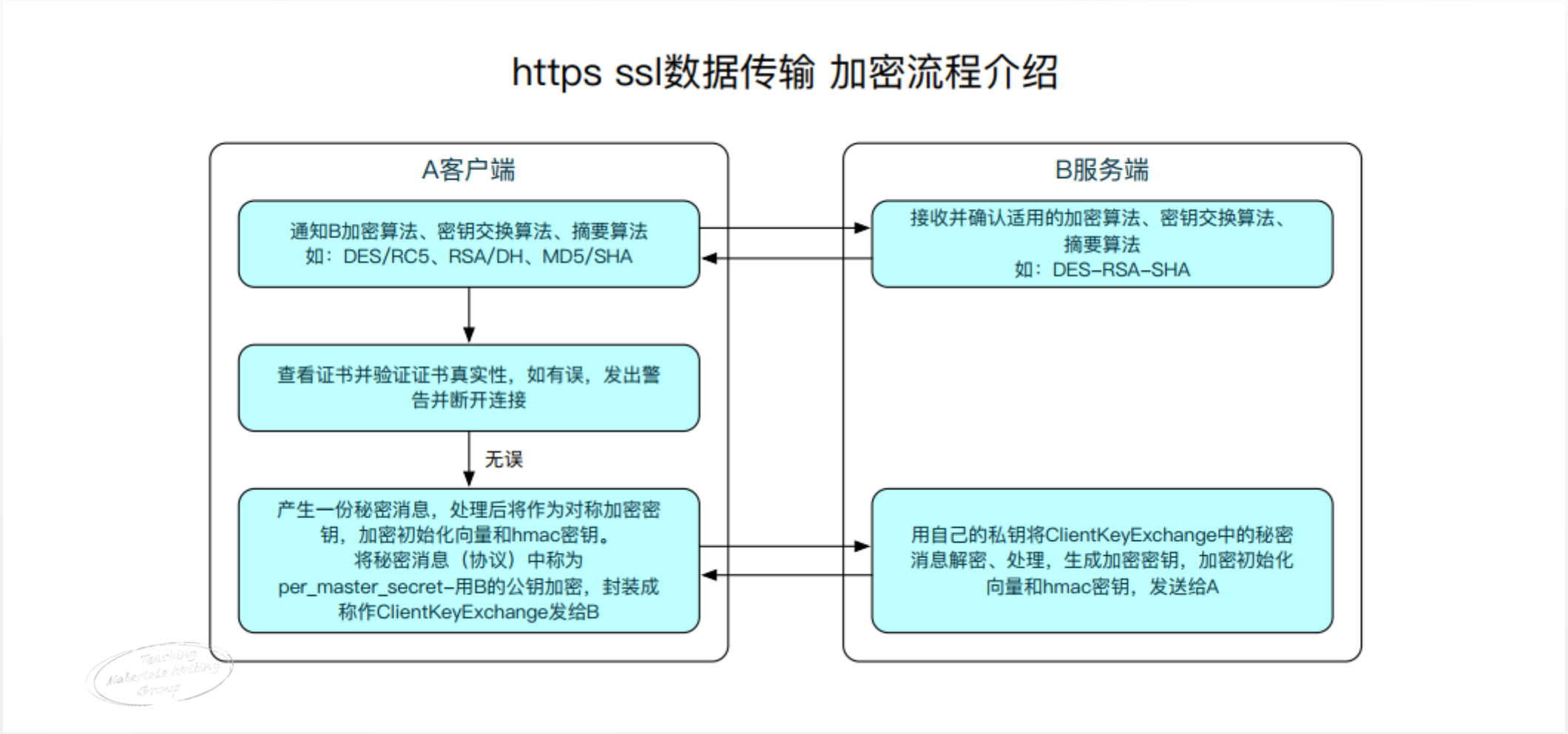
- 密码学中应用最为广泛的的三类算法：

✓ 对称算法（分组密码算法）代表分组密码算法（国际DES和国密SM4）

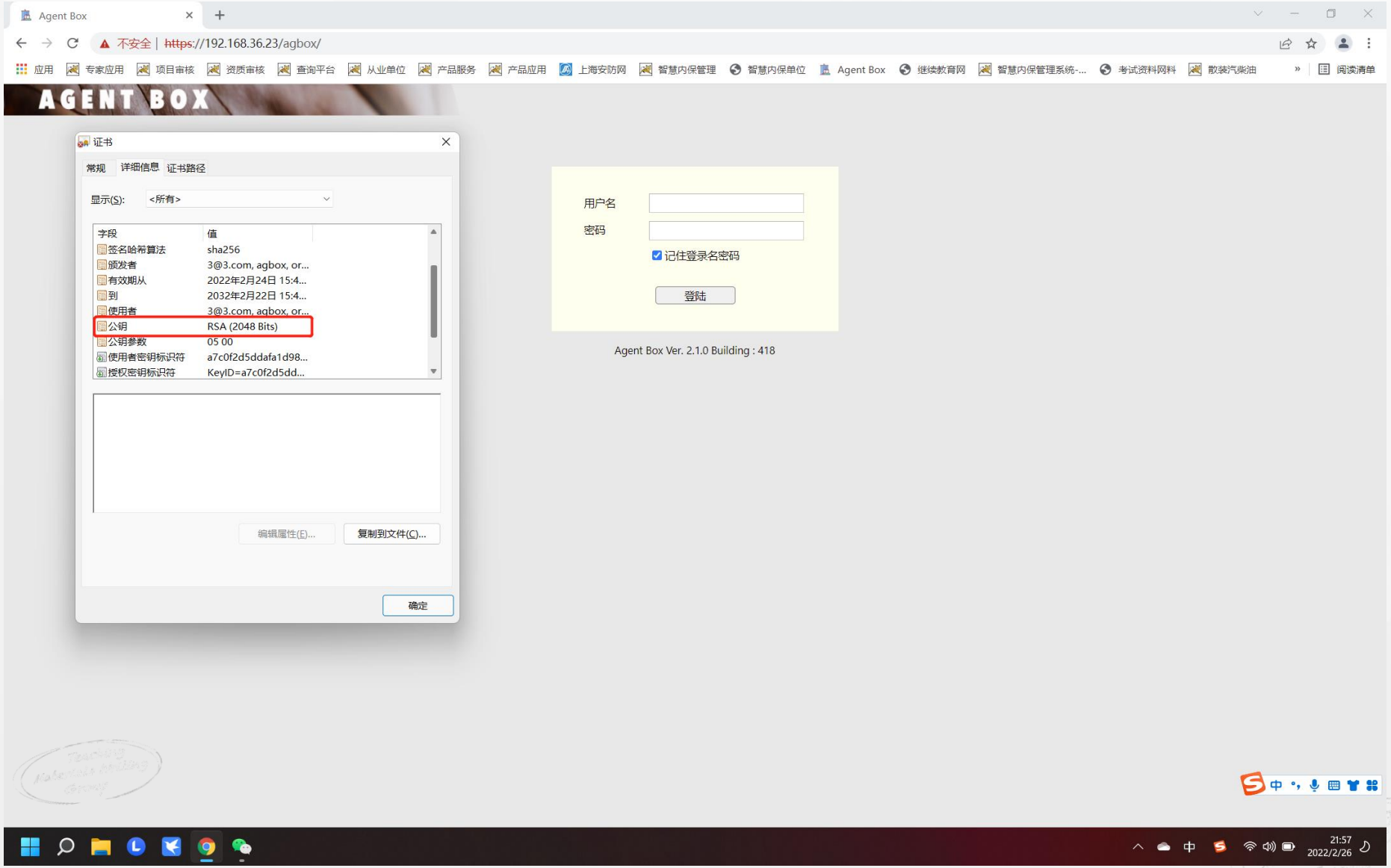
✓ 非对称算法（公钥密码算法）代表公钥密码算法（国际RSA和国密SM2 ）

✓ 杂凑算法（摘要算法）代表摘要算法（国际SHA-256系列和国密SM3 ）

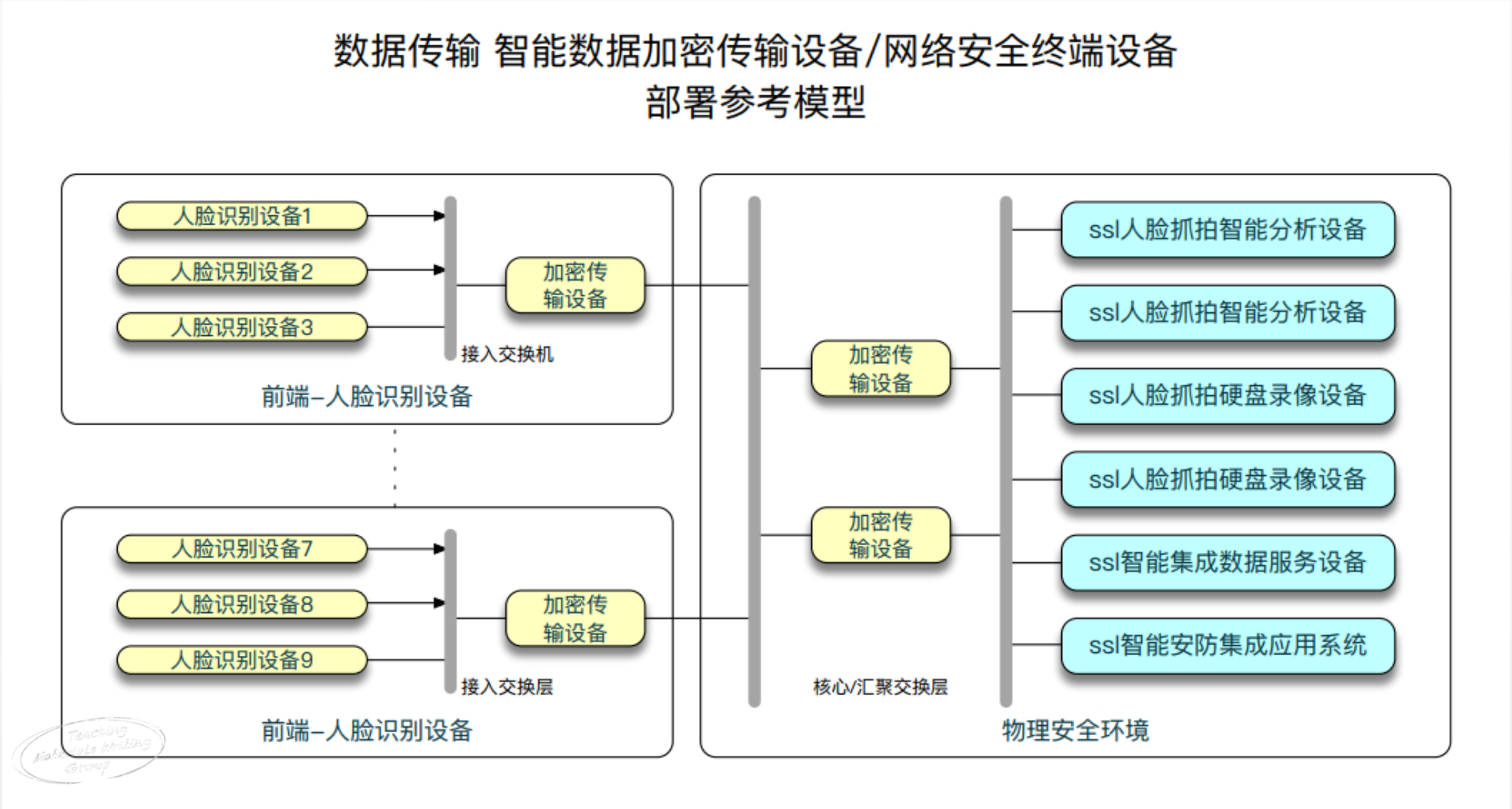
六 传输要求


https ssl数据传输 加密流程介绍
A客户端
B服务端
通知B加密算法、密钥交换算法、摘要算法
如：DES/RC5、RSA/DH、MD5/SHA
接收并确认适用的加密算法、密钥交换算法、
摘要算法
如：DES-RSA-SHA
查看证书并验证证书真实性，如有误，发出警
告并断开连接
无误
产生一份秘密消息，处理后将作为对称加密密
钥，加密初始化向量和hmac密钥。
将秘密消息（协议）中称为
per_master_secret-用B的公钥加密，封装成
称作ClientKeyExchange发给B
用自己的私钥将ClientKeyExchange中的秘密
消息解密、处理，生成加密密钥，加密初始化
向量和hmac密钥，发送给A

六 传输要求


Agent Box
不安全 | https://192.168.36.23/agbox/
AGENT BOX
证书
常规
详细信息
证书路径
显示(S): <所有>
字段
值
签名哈希算法 sha256
颁发者 3@3.com, agbox, or...
有效期从 2022年2月24日 15:4...
到 2032年2月22日 15:4...
使用者 3@3.com, agbox, or...
公钥 RSA (2048 Bits)
公钥参数 05 00
使用者密钥标识符 a7c0f2d5ddafa1d98...
授权密钥标识符 KeyID=a7c0f2d5dd...
编辑属性(E)...
复制到文件(C)...
确定
用户名
密码
记住登录名密码
登陆
Agent Box Ver. 2.1.0 Building : 418
21:57
2022/2/26

六 传输要求


数据传输 智能数据加密传输设备/网络安全终端设备
部署参考模型
人脸识别设备1
人脸识别设备2
人脸识别设备3
加密传输设备
接入交换机
前端–人脸识别设备
人脸识别设备7
人脸识别设备8
人脸识别设备9
加密传输设备
接入交换层
前端–人脸识别设备
加密传输设备
加密传输设备
核心/汇聚交换层
ssl人脸抓拍智能分析设备
ssl人脸抓拍智能分析设备
ssl人脸抓拍硬盘录像设备
ssl人脸抓拍硬盘录像设备
ssl智能集成数据服务设备
ssl智能安防集成应用系统
物理安全环境

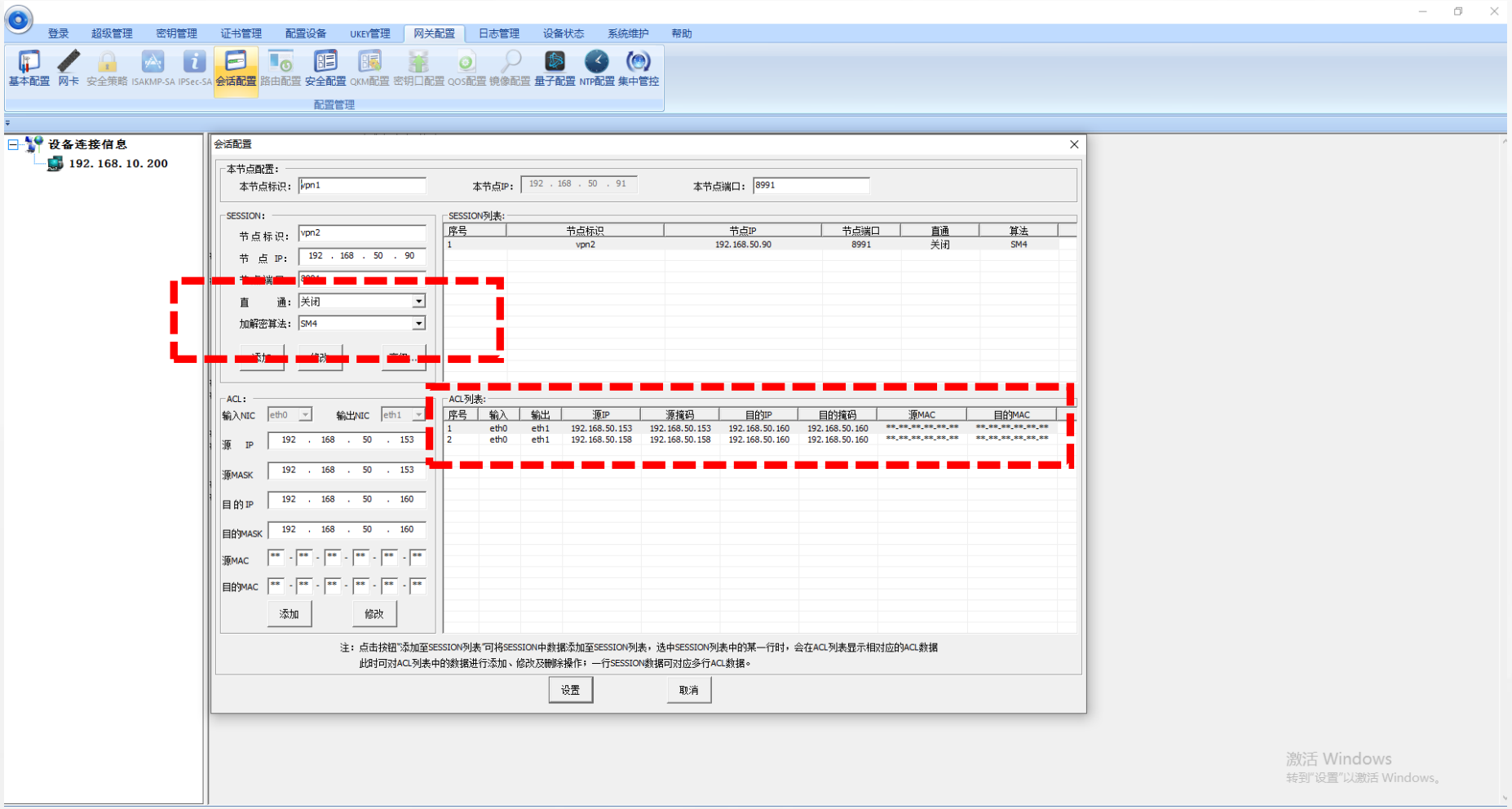
六 传输要求

六 传输要求


首页 网络 防火墙 网关 服务 日志 状态 工具 管理
关机
非国标代理网关设置
网关联网参数配置
本网关参数设置
sipID: 31000000001180000003
ip地址: 192.168.4.143
sip端口: 5065
国密设备证书
浏览
序列号：00cb3cb0622be803c1
颁发给：flyfish
颁发者：Beijing
有效期：2021-10-2 到 2031-10-1
内网国标服务器参数设置
IP地址: 192.168.4.104
sipID: 31000000002000000001
sip端口: 5060
用户名: 31000000001180000003
心跳时间: 60
国标平台类型: 0
国密服务器证书
浏览
序列号：7181404a
颁发给：TEST
颁发者：ST
有效期：2018-10-14 到 2028-10-11
密码: 123456
失效时间: 3600
默认值:0,其他值请咨询技术支持
保存


首页 网络 防火墙 网关 服务 日志 状态 工具 管理
关机
非国标代理网关设置
网关联网参数配置
服务器地址: 192.168.4.143
签名算法: SM2
加密算法: SM4
保存

六 传输要求



六 传输要求

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

7 人脸识别数据传输要求

7.1 人脸识别应采用数据结构独立的专用网络（可采用 VLAN 的独立网段），应对系统中所有接入设备的网络端口予以管理和绑定。

7.2 人脸识别相关数据内容关联应用终端的所有 USB 端口应采用可通过出入口控制系统授权刷卡认证的 USB 防拔插设备予以绑定管理，并不应通过互联网与其他应用实现实时联网。

关注点 9

人脸识别数据传输基本要求

- 网络端口要求

人脸识别数据端口基本要求

- 数据端口要求

六 传输要求

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

7.3 人脸验证和人脸辨识在采集端完成人脸识别数据采集并在服务器端完成人脸识别的，系统建设应满足《信息安全技术远程人脸识别系统技术要求》（GB/T 38671）的相关要求。

7.4 人脸识别由与其相关数据内容关联应用终端（含软件）所构成系统的，系统建设应满足《信息安全技术远程人脸识别系统技术要求》（GB/T 38671）相关要求。

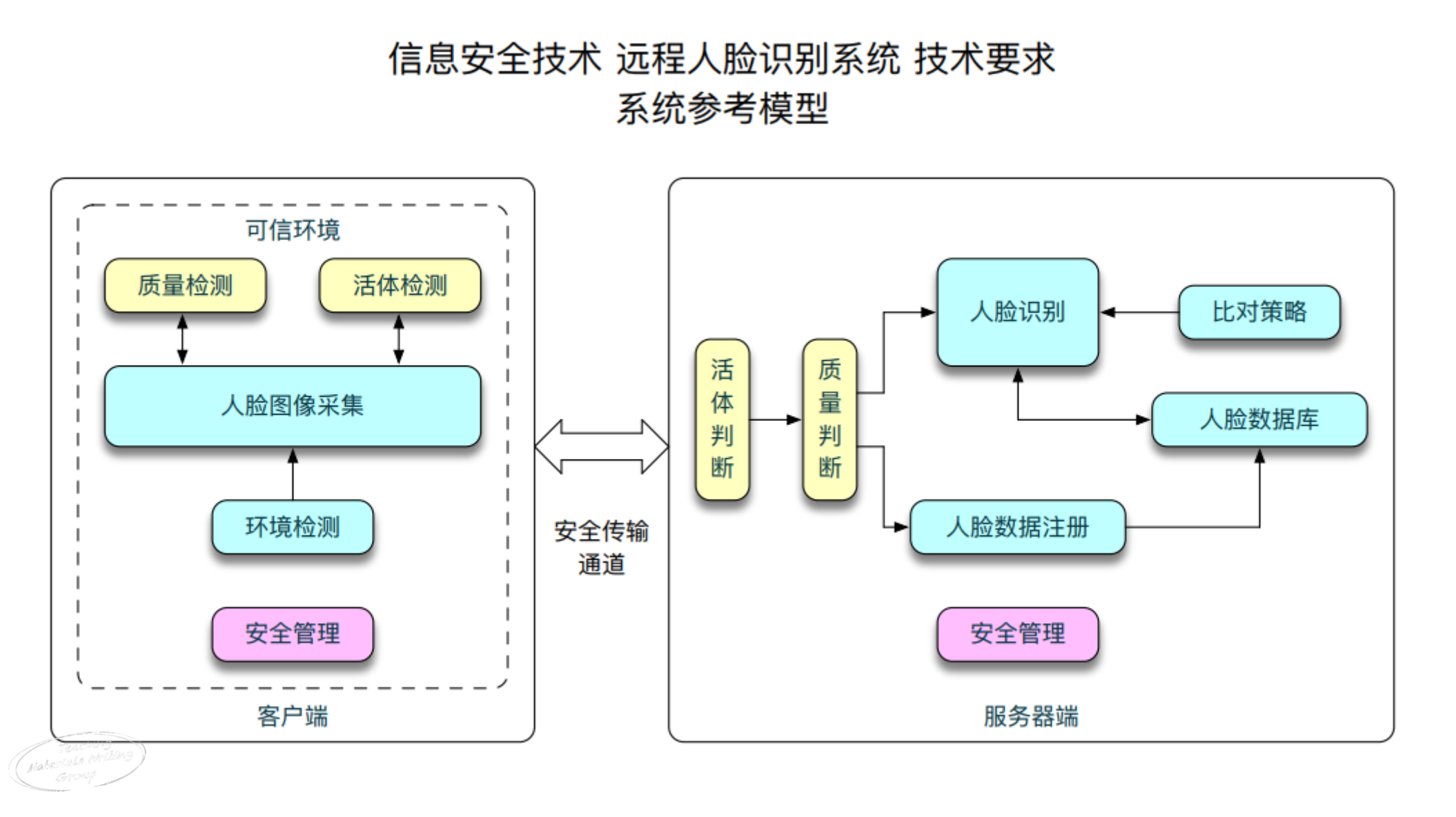
7.5 除用于维护所提供的产品或服务的安全稳定运行所必须，以及智能分析结果数据外，人脸识别数据、个人身份信息不应在智能集成数据服务设备、智能安防集成应用系统体现或展示，对确有除此以外应用需求的，系统建设应满足《信息安全技术 远程人脸识别系统技术要求》（GB/T 38671）的相关要求。

关注点 10

远程人脸识别

- 远程人脸识别系统由客户端、服务端、安全传输通道组成，系统由客户端实现人脸的采集，经安全传输通道传输，在服务器端远程进行比对。

六 传输要求


信息安全技术 远程人脸识别系统 技术要求
系统参考模型
可信环境
质量检测
活体检测
人脸图像采集
环境检测
安全管理
客户端
安全传输
通道
活体判断
质量判断
人脸识别
比对策略
人脸数据库
人脸数据注册
安全管理
服务器端

七 评审要点

评审关注要点

- 自2022年3月1日起本市安全技术防范工程系统中使用带人脸识别的安防产品，除符合现行标准规范要求外，还应符合《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求》（以下简称《技术要求》）。

✓ 自2022年3月1日起，评审过程中，专家应根据《技术要求》认真核查申报项目的设计内容、系统架构，关注带人脸识别系统的数据传输是否符合要求，对不符合《技术要求》的应提出修改意见；应告知设计施工单位及建设使用单位与本项目相关带人脸识别产品的技术要求，并明确验收时检验机构及验收专家将对系统架构及其性能和系统指标进行检验、查验。

✓ 自2022年4月1日起，设计施工单位提交安全技术防范工程评审时，带人脸识别的安防产品应提供相应的检测报告。

八 验收要点

验收关注要点

- 自2022年3月1日起本市安全技术防范工程系统中使用带人脸识别的安防产品，除符合现行标准规范要求外，还应符合《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求》（以下简称《技术要求》）。

✓ 自2022年3月1日起，申报并取得通过评审的安全技术防范工程，项目验收时，检验机构将对其性能和系统指标进行检验。

八 验收要点


人脸识别
工程查验
信息安全要求
身份鉴别要求（工程查验）
访问控制要求（工程查验）
安全审计要求（工程查验）
验证辨识要求
采集告知明示（工程查验）
删除原证照片（工程查验）
验证查询、辨识查询
防伪攻击能力（工程查验）
人脸照片、纸质面具、人脸视频、人脸合成
数据信息隔离（工程查验）
到期自动清理（工程查验）
到期自动删除、匿名化处理
人脸分析要求
去重处理要求（工程查验）
连续去重、间断去重
预警提示应用（工程查验）
数据信息隔离（工程查验）
到期自动清理（工程查验）
到期自动删除
数据传输要求
专用独立网络（工程查验）
人脸验证、人脸辨识、人脸分析
数据端口绑定（工程查验）

Thank you!