ICS 35.240.15
L 64

中华人民共和国国家标准

GB/T 38851—2020

信息技术　识别卡
集成指纹的身份识别卡通用技术要求

Information technology—Identification cards—
General technical requirements for integrated fingerprint identification card

2020-07-21 发布　　2021-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准起草单位:中国电子技术标准化研究院、楚天龙股份有限公司、华大半导体有限公司、上海一芯智能科技有限公司、深圳赛西信息技术有限公司、北京中电华大电子设计有限责任公司、北京智芯微电子科技有限公司、金邦达有限公司、东信和平科技股份有限公司、飞天诚信科技股份有限公司、天津市红天科技发展有限公司、北京眼神科技有限公司、北京握奇数据股份有限公司、大唐微电子技术有限公司、中电智能卡有限责任公司、紫光同芯微电子有限公司、军事科学院系统工程研究院后勤科学与技术研究所、上海复旦微电子集团股份有限公司、上海密特印制有限公司、中国银联股份有限公司、中国科学院自动化研究所、国民技术股份有限公司。

本标准主要起草人:曹国顺、兰天、蒋曲明、王峻峰、李丹、余晖、付青琴、徐木平、原爱阳、周向涛、朱鹏飞、邴志刚、宋方方、张树蕊、白婧、余恒亦、周峥、王进、曹宇、胡波、秦潮、邵兴、吴行宇、刘晓晨、高伟、徐平江、程旺迟、张建伟、续素芬。

信息技术　识别卡
集成指纹的身份识别卡通用技术要求

1　范围

本标准规定了集成指纹的身份识别卡(以下简称指纹身份识别卡)的基本组成、外观与结构、机械适应性、环境适应性、电特性与传输协议、通用流程与基本功能性能、命令、信息安全等要求。

本标准适用于指纹身份识别卡的研发、生产、检验和使用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 14916—2006　识别卡　物理特性

GB/T 16649.1—2006　识别卡　带触点的集成电路卡　第1部分:物理特性

GB/T 16649.2　识别卡　带触点的集成电路卡　第2部分:触点的尺寸和位置

GB/T 16649.3　识别卡　带触点的集成电路卡　第3部分:电信号和传输协议

GB/T 16649.10　识别卡　带触点的集成电路卡　第10部分:同步卡的电信号和复位应答

GB/T 16649.11—2019　识别卡　集成电路卡　第11部分:通过生物特征识别方法的身份验证

GB/T 17554.1—2006　识别卡　测试方法　第1部分:一般特性测试

GB/T 17554.3—2006　识别卡　测试方法　第3部分:带触点的集成电路卡及其相关接口设备

GB/T 26237.1　信息技术　生物特征识别数据交换格式　第1部分:框架

GB/T 26237.2　信息技术　生物特征识别数据交换格式　第2部分:指纹细节点数据

GB/T 26237.3　信息技术　生物特征识别数据交换格式　第3部分:指纹型谱数据

GB/T 26237.4　信息技术　生物特征识别数据交换格式　第4部分:指纹图像数据

GB/T 26572—2011　电子电气产品中限用物质的限量要求

GB/T 26704—2011　铅笔

GB/T 33767.1—2017　信息技术　生物特征样本质量　第1部分:框架

ISO/IEC 10373-3　识别卡　测试方法　第3部分:带触点的集成电路卡及其相关接口设备(Identification cards—Test methods—Part 3:Integrated circuit cards with contacts and related interface devices)

ISO/IEC 10373-6　识别卡　测试方法　第6部分:接近式卡(Identification cards—Test methods—Part 6:Proximity cards)

ISO/IEC 10373-7　识别卡　测试方法　第7部分:邻近式卡(Identification cards—Test methods—Part 7:Vicinity cards)

ISO/IEC 14443(所有部分)　识别卡　无触点的集成电路卡　接近卡式(Identification cards—Contactless integrated circuit cards—Proximity cards)

ISO/IEC 30107(所有部分)　信息技术　生物特征识别呈现攻击检测(Information technology—Biometric presentation attack detection)

3 术语和定义

下列术语和定义适用于本文件。

3.1

ID-1

标称尺寸为：宽度 85.60 mm，高度 53.98 mm，厚度 0.76 mm。

[GB/T 14916—2006，定义 4.5]

3.2

指纹身份识别卡 fingerprint identification card

具有卡上指纹采集功能、用于标识用户身份的凭证。

3.3

指纹特征 fingerprint feature

从指纹样本中提取的，用于比对的数值或标记的集合。

[GB/T 37045—2018，定义 3.5]

3.4

指纹模板 fingerprint template

被存储的、在比对时作为参考的指纹特征的集合。

[GB/T 37045—2018，定义 3.6]

3.5

呈现攻击 presentation attack

以干扰指纹特征识别系统的操作为目的，针对指纹特征数据采集模块的一种攻击行为。

[GB/T 37036.1—2018，定义 3.3]

3.6

呈现攻击检测 presentation attack detection

对呈现攻击的自动检测。

[GB/T 37036.1—2018，定义 3.4]

3.7

质量 quality

指纹特征样本满足目标应用的指定条件的程度。

注：指定的质量条件可涉及几方面，例如，影像清晰度、分辨率等。隐式质量条件决定获得正确匹配结果的可能性。

[GB/T 37036.1—2018，定义 3.5]

3.8

质量判断 quality judgment

对指纹特征样本质量是否满足目标应用指定条件的检验过程。

[GB/T 37036.1—2018，定义 3.6]

3.9

运行环境 execution environment

存在于设备中的软硬件集合，为应用程序在移动设备中的运行提供必要的能力支持。

注：一般包括硬件处理单元、易失性存储单元、非易失性存储单元、操作系统和调用接口等组件。

3.10

可信运行环境 trusted execution environment

存在于设备中的受控运行环境，具备较强的安全保护能力，以确保运行其中的应用程序、敏感数据

等得到安全的存储、处理和保护。

4 缩略语

下列缩略语适用于本文件。

COS:片上操作系统(Chip OS)

FAR:错误接受率(False Accept Rate)

FRR:错误拒绝率(False Reject Rate)

LED:发光二极管(Light Emitting Diode)

5 基本组成

指纹身份识别卡模块框图如图 1 所示。

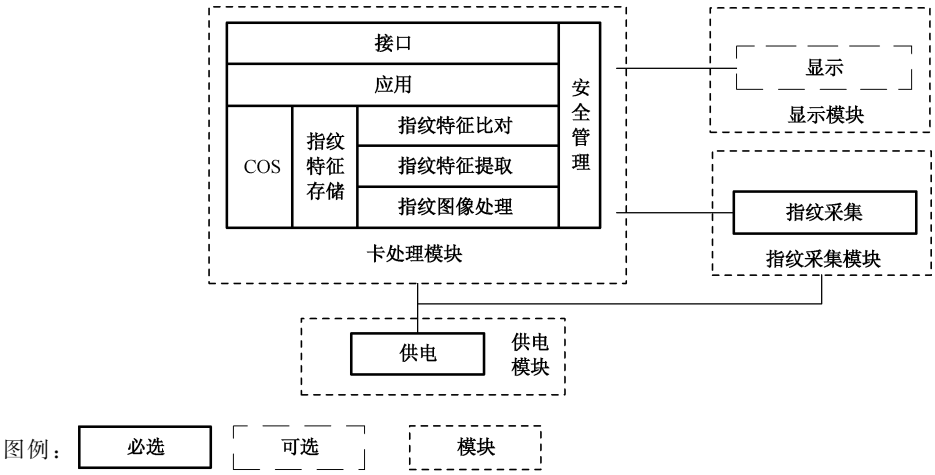

图 1 指纹身份识别卡模块框图

指纹身份识别卡可包括以下模块:

——指纹采集模块,必选,用于实现指纹感知采集功能,支持通过硬件接口和指纹处理模块通信。指纹采集可采用电容传感器技术、超声波传感器技术、光学传感器技术或其他技术。

——卡处理模块,必选,提供指纹处理的软硬件环境,用于实现指纹图像处理、指纹特征提取、指纹特征比对、指纹特征存储,以及安全管理和应用。指纹处理模块支持通过接触接口、非接触接口等与外部设备通信,同时具有与指纹采集模块之间的通信接口。

——供电模块,必选,用于为指纹身份识别卡提供电源,供电方式可包括触点供电、线圈感应供电、电池供电等。

——显示模块,可选,用于提示指纹处理状态等信息,例如显示屏或 LED 灯。

6 外观与结构

本标准规定的指纹身份识别卡,外观与结构要求如下:

a) 外观要素构成:

1) 带接触接口的指纹身份识别卡正面应包括以下要素:触点、指纹采集区,通信和验证状态提示(可选);背面无特别要求。

2) 不带接触接口的指纹身份识别卡正面应包括以下要素：指纹采集区，通信和验证状态提示（可选）；背面无特别要求。

b) 指纹采集区表面与其附近的卡表面之间的高度差，向上应不超过 0.05 mm，向下应不超过 0.10 mm。

c) 整卡应采用封闭紧固封装，除了卡上指纹采集模块和对外通信接口外，不应留有其他可被直接接触探测的无覆盖区域。

d) 整卡应使用拆解存迹的涂层或覆盖材料，以阻止直接观察，并可提供拆卸或移动内部部件的证据。

e) ID-1 规格指纹身份识别卡外观与结构应同时符合 GB/T 14916—2006 的规定，卡面布局示例参见附录 A。

f) 针对有源指纹身份识别卡，卡面宜有环保回收提示信息。

7 机械适应性

7.1 弯曲韧性

ID-1 规格指纹身份识别卡按照 GB/T 17554.1—2006 中 5.7 规定的方法测试，变形最大值应为 25 mm，最小值应为 10 mm。在移开测试装置后的 1 min 内，卡应恢复其初始平面状态（偏移在 1.5 mm 内）。

7.2 动态弯曲应力

ID-1 规格指纹身份识别卡在进行 GB/T 17554.1—2006 中 5.8 规定的动态弯曲应力测试 200 次之后，卡应保持其功能并应不出现开裂。

7.3 动态扭曲应力

ID-1 规格指纹身份识别卡在进行 GB/T 17554.1—2006 中 5.9 规定的动态扭曲应力测试 1 000 次之后，卡应保持其功能并应不出现开裂。

7.4 机械强度

卡应能抵抗对其表面及其任何组成部件的损害，并在正常使用、保存和处理过程中保持完好。

对于 ID-1 规格指纹身份识别卡，指纹采集区在直径 1 mm 的钢球施加 1.5 N 的工作压力下，持续时间 1 min 不应被破坏，其他区域（包括触点），参见 GB/T 17554.3—2006 中附录 A.1 规定的方法测试，卡不应被破坏。

7.5 耐划痕

指纹身份识别卡应能抵抗对其表面触点和指纹采集区不低于 2H 强度的刮擦损害，2H 的定义见 GB/T 26704—2011 的表 1。

8 环境适应性

8.1 限用物质的限量

卡在正常使用中不应存在毒性危害。应符合 GB/T 26572—2011 的要求。

8.2 耐化学性

应符合 GB/T 17554.1—2006 中 5.4 的要求。

8.3 温、湿度条件下的卡尺寸稳定性和翘曲

ID-1 规格的卡应符合 GB/T 14916—2006 中 8.5 的要求。

8.4 光

应符合 GB/T 14916—2006 中 8.6 的要求。

8.5 剥离强度

ID-1 规格的卡应符合 GB/T 14916—2006 中 8.8 的要求。

8.6 粘连或并块

应符合 GB/T 14916—2006 中 8.9 的要求。

8.7 全卡翘曲

ID-1 规格的卡应符合 GB/T 14916—2006 中 8.11 的要求。

8.8 抗热度

ID-1 规格的卡应符合 GB/T 14916—2006 中 8.12 的要求。

8.9 表面畸变

ID-1 规格的卡应符合 GB/T 14916—2006 中 8.13 的要求。

8.10 污染和卡部件的相互影响

应符合 GB/T 14916—2006 中 8.14 的要求。

8.11 紫外线

应符合 GB/T 16649.1—2006 中 4.2.1 的要求。

8.12 X 射线

应符合 GB/T 16649.1—2006 中 4.2.2 的要求。

8.13 静态磁场

在 640 kA/m 的静态磁场内暴露后，指纹身份识别卡应能继续正常工作。

8.14 交变磁场

指纹身份识别卡，若带有非接触接口，在频率为 13.56 MHz、磁场强度平均值(RMS)为 7.5 A/m 的 1.33 倍(4/3 倍)、磁场强度最大值(RMS)不超过 7.5 A/m 的 1.6 倍(8/5 倍)的交变磁场内，在任意方向上持续暴露(时间不低于 30 s)后，指纹身份识别卡应能继续正常工作。

8.15 静电

按照 ISO/IEC 10373-3 中所描述的静电测试方法，卡接触触点和地之间，由一个 100 pF 电容经过

1 500 Ω 放电产生 2 kV 的静电，卡暴露其中，其功能不应降低。卡指纹采集区和地之间，由一个 100 pF 电容经过 1 500 Ω 放电产生 6 kV 的静电，卡暴露其中，其功能不应降低。

其他区域依据 ISO/IEC 10373-6 和 ISO/IEC 10373-7 中描述的静电试验方法，试验电压为 4 kV 时，卡应继续按照试验运行。

9 电特性与传输协议

具有接触接口的指纹身份识别卡，接触接口的电特性与传输协议应遵循 GB/T 16649.1—2006、GB/T 16649.2、GB/T 16649.3、GB/T 16649.10 的规定。

具有非接触接口的指纹身份识别卡，非接触接口的电特性与传输协议应遵循 ISO/IEC 14443 的规定。

10 通用流程与基本功能、性能要求

10.1 通用流程

10.1.1 指纹登记

10.1.1.1 卡上登记指纹

使用指纹身份识别卡卡上登记指纹的过程，包括如下步骤：

a) 用户在指纹身份识别卡上启动指纹登记过程；
b) 用户通过指纹身份识别卡的指纹采集模块采集用户指纹图像样本；
c) 指纹身份识别卡完成指纹图像样本的质量判断和呈现攻击检测后，提取用户指纹特征项，然后将该用户指纹特征项存储在安全运行环境中作为该用户的指纹模板，并与用户身份标识关联起来；
d) 结束指纹登记过程。

10.1.1.2 卡外登记指纹

使用外置专用指纹设备登记指纹的过程，包括如下步骤：

a) 用户将指纹身份识别卡和外置专用指纹设备相连接，启动指纹登记过程；
b) 外置专用指纹设备采集用户指纹图像样本，通过安全通道将指纹图像样本传输到指纹身份识别卡卡内；
c) 指纹身份识别卡完成指纹图像样本的质量判断和呈现攻击检测后，提取用户指纹特征项，然后将该用户指纹特征项存储在安全运行环境中作为该用户的指纹模板，并与用户身份标识关联；
d) 结束指纹登记过程。

10.1.2 指纹识别

指纹识别是将“采集的用户指纹”与“登记的用户指纹”进行比对，以完成持卡人识别的过程。包括如下步骤：

a) 用户在指纹身份识别卡上启动指纹识别过程；
b) 指纹身份识别卡上的指纹采集模块采集用户指纹图像样本，完成质量判断和呈现攻击检测后，提取用户指纹特征项；
c) 指纹身份识别卡将提取的用户指纹特征项与存储在卡上的指纹模板进行比对；
d) 指纹身份识别卡根据比对结果进行持卡人识别，并将结果输出；

e) 结束识别过程。

10.1.3 指纹注销

指纹注销是用户删除指纹身份识别卡上已登记指纹模板及其附属敏感信息的过程。包括如下步骤：

a) 用户在指纹身份识别卡上启动指纹注销过程；
b) 指纹身份识别卡验证用户身份，验证身份方式可以是识别指纹、验证密码等；
c) 用户身份验证通过后，指纹身份识别卡删除与用户关联的指纹模板及指纹模板附属敏感信息；
d) 结束指纹注销过程。

10.2 基本功能要求

指纹身份识别卡应包括但不限于如下功能：

a) 应至少支持如下两种登记功能中的一种，宜两种都支持：基于外置终端指纹采集的指纹登记功能、基于卡上指纹采集的指纹登记功能。
b) 应支持对已登记指纹的更新和注销功能。
c) 应支持卡上指纹识别功能。
d) 应支持卡上指纹 360°可识别。
e) 应具有明确的用户提示，告知用户对其指纹样本进行了采集。
f) 应能对获得的指纹样本进行质量判断，以确定当前指纹特征样本是否满足指纹识别处理的需求。宜支持对指纹样本质量指标进行设定。指纹特征样本未通过质量判断时应具备相应的处理机制，如提示用户重新采集或提示失败等。质量判断的依据应符合 GB/T 33767.1—2017 对样本质量的要求。
g) 应能对获得的指纹图像样本进行呈现攻击检测，以防止恶意伪造。宜支持对呈现攻击检测准确率指标进行设定。检测出呈现攻击时应具备相应的处理机制，如失败/错误提示或进行风险提示等。呈现攻击检测应遵循 ISO/IEC 30107 的规定。
h) 已登记的指纹，应在扩展项中增加事件标识符、唯一设备标识符、登记日期和时间等数据。数据交换应遵循 GB/T 26237.1，并遵循 GB/T 26237.2 或 GB/T 26237.3 或 GB/T 26237.4 中的规定。
i) 应具备异常情况处理能力，包括但不限于指纹采集失败、指纹登记失败、指纹删除失败和指纹比对失败后的处理机制。

10.3 基本性能要求

指纹身份识别卡基本性能要求如下：

a) 指纹身份识别卡上可登记指纹数量不小于 2 个。
b) 指纹登记时，在良好供电情况下，单次采集完成的时间应小于或等于 3 000 ms。1∶1 识别场景中，单次指纹识别时间应小于或等于 1 000 ms。单次指纹识别包括完成一次指纹采集、单个指纹特征比对、比对结果输出的过程。
c) 宜支持对 FAR 和 FRR 等性能指标进行设定。指纹识别的准确性应至少满足如下指标：当 FAR 为 1/10 000 时，FRR 应小于或等于 5%。
d) 指纹身份识别卡使用寿命应大于或等于 10 万次指纹识别。

由卡内电池供电的指纹身份识别卡卡内电池应满足如下要求：能够保证指纹身份识别卡工作 3 年以上或支持不低于 7 000 次有源指纹识别操作，有源指纹识别操作定义为通过卡内置电池供电完成的操作。

11 命令

基于外置指纹采集终端的指纹登记应使用 GB/T 16649.11—2019 的表 3 中定义的 STORE BIOMETRIC REFERENCE 命令。

基于卡上指纹采集的指纹登记宜使用 GB/T 16649.11—2019 的表 3 中定义的 CAPTURE AND STORE BIOMETRIC REFERENCE 命令。

指纹识别宜使用 GB/T 16649.11—2019 的表 3 中定义的 CAPTURE AND COMPARE BIOMETRIC PROBE 命令。

基于外置指纹采集终端的已登记指纹的更新应使用 GB/T 16649.11—2019 的表 3 中定义的 UPDATE BIOMETRIC REFERENC 命令。

基于卡上指纹采集的已登记指纹的更新宜使用 GB/T 16649.11—2019 的表 3 中定义的 CAPTURE AND UPDATE BIOMETRIC REFERENCE 命令。

对已登记指纹的注销宜使用 GB/T 16649.11—2019 的表 3 中定义的 UPDATE BIOMETRIC REFERENCE 命令。命令中的生物特征数据模板、生物特征信息模板及生物特征信息模板组模板应为随机生成的数据，不宜使用固定数据(包括但不限于全‘0’、全‘1’)。

注：指纹注销时，指纹身份识别卡内的相应数据被 UPDATE BIOMETRIC REFERENCE 命令中的数据覆盖，从而使已登记的指纹不可用。

12 信息安全

12.1 一般要求

一般要求包括但不限于：

a) 指纹身份识别卡应具备明确的卡实体边界。指纹的采集可在卡实体外或卡实体内完成，指纹图像的处理、指纹模板的存储和比对功能均应在卡实体内完成；相关功能的安全保护机制也应包含在卡实体内。

b) 指纹身份识别卡和卡外实体通过通信接口交互敏感数据时，宜采用安全通道机制以保证交互数据的完整性和机密性。

c) 指纹身份识别卡应具备鉴别机制和访问控制机制，以验证卡外实体的身份合法性并限定其操作权限。

d) 指纹身份识别卡的软件均应运行在卡实体内部，应具备完整性保护机制保障软件不被篡改。

e) 指纹身份识别卡硬件及卡内软件构成可信运行环境，该环境不应受卡外部运行环境的干扰。

f) 指纹身份识别卡应采用整卡紧固封闭封装，以防止对卡内部未授权的探测和访问。

12.2 指纹采集和处理安全

指纹采集和处理安全包括但不限于：

a) 指纹采集模块不应留存指纹样本等敏感信息；

b) 指纹采集模块不应干扰指纹处理模块的执行；

c) 应及时清除未通过质量判断的指纹样本，并确保其不可恢复；

d) 指纹特征项提取结束后，应及时清除缓存中的指纹样本，并确保其不可恢复；

e) 卡外向卡内传递指纹图像样本时，应保障样本的机密性和完整性。

12.3 指纹存储安全

指纹存储安全包括但不限于：

a) 指纹模板存储过程应在卡内可信运行环境中执行；

b) 应防止对指纹模板的非授权访问和篡改；

c) 应保护已登记指纹模板与用户标识之间的正确关联关系，防止被非法修改；

d) 宜采用加密方式对指纹模板进行存储；

e) 对操作过程产生的临时数据，应及时清除并确保其不可恢复；

f) 对已删除的指纹模板，应及时清除并确保其不可恢复。

12.4 指纹比对安全

指纹比对安全包括但不限于：

a) 指纹比对过程应在卡内可信运行环境中执行；

b) 应采取有效的安全机制，保护比对过程不被干扰和旁路攻击；

c) 比对结束后，应及时清除缓存中的指纹特征数据和比对过程中所产生的其他临时数据；

d) 应设定比对失败尝试次数限制，并提供超过限制次数后的保护措施；

e) 应采取有效的安全机制，确保识别结果的完整性，不被非法篡改。

附 录 A
（资料性附录）
ID-1 规格指纹身份识别卡卡面布局

对于带接触接口的 ID-1 规格指纹身份识别卡，正面包括以下要素：接触触点、指纹采集区域。如图 A.1 所示。

对于非接触接口的 ID-1 规格指纹身份识别卡，正面包括以下要素：指纹采集区域。

ID-1 规格指纹身份识别卡背面无特别要求。

指纹身份识别卡指纹采集区布局参数如表 A.1 所示。

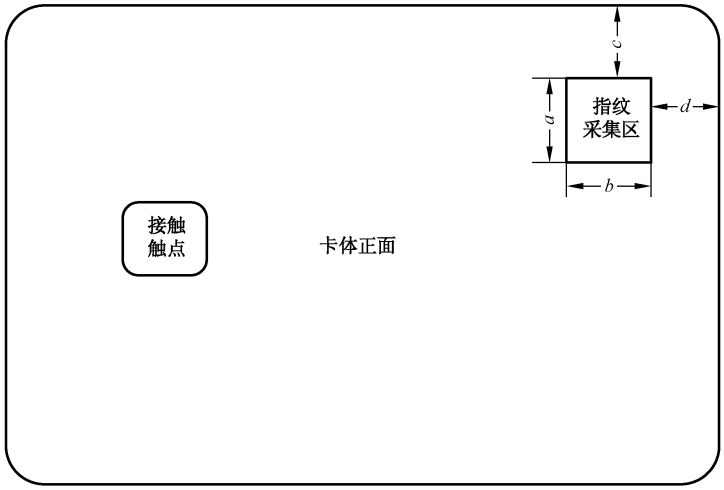

图 A.1 带接触接口的指纹身份识别卡正面布局图

表 A.1 指纹身份识别卡指纹采集区布局参数

单位为毫米

参数	值
指纹采集区长度 a	16.0±0.10
指纹采集区宽度 b	16.0±0.10
指纹采集区距离卡的上边沿 c	10.4±0.10
指纹采集区距离卡的右边沿 d	5.25±0.10

参 考 文 献

[1] GB/T 37036.1—2018 信息技术 移动设备生物特征识别 第1部分:通用要求
[1] GB/T 37045—2018 信息技术 生物特征识别 指纹处理芯片技术要求