ICS 33.030
CCS M 21

团　体　标　准

T/TAF 226—2024

面向移动互联网产品的用户安全隐私感体验评估实施指南

Implementation guidance for user security and privacy experience evaluation for mobile Internet products

2024-05-13 发布　　2024-05-13 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：荣耀终端有限公司、中国信息通信研究院、泰尔认证中心有限公司、蚂蚁科技集团股份有限公司、北京快手科技有限公司、OPPO广东移动通信有限公司、华为技术有限公司、北京三星通信技术研究有限公司、维沃移动通信有限公司、中兴通讯股份有限公司、北京微梦创科网络技术有限公司、阿里巴巴(中国)有限公司、小米通讯技术有限公司、厦门美柚股份有限公司、武汉安天信息技术有限责任公司、安谋科技（中国）有限公司。

本文件主要起草人：于洪健、赵晓娜、王艳红、关福生、宁华、陈鑫爱、林键、张艳梅、李辰淑、常琳、周飞、李可心、林冠辰、落红卫、王昕、李腾、李实、潘洁、吴越、贾科、潘万鹏、任资政、邹庆、黄天宁、王响、黄鹏华、余丽娜、葛伟、王天。

引　言

移动互联网产品由于其功能的多样性和开放性，往往面临网络与信息安全、隐私保护等诸多问题，容易对用户使用中的安全隐私感体验造成影响。随着国内外网络安全、数据安全、个人信息保护等相关基础法律法规相继出台，安全与隐私保护越来越成为全社会关注的焦点，企业和用户越来越重视移动互联网产品的安全与隐私保护理念与设计。

目前，移动互联网产品提供者在构建安全隐私感设计模型时，往往结合社会心理学研究结论，从确定感和控制感两个需求层次进行设计，但是，行业内尚无统一有效的用户安全隐私感体验评估方法或标准供企业作参考。

因此，本文件旨在提出一套通用的用户安全隐私感体验评估指标体系设计与使用指导标准，方便企业对自身产品的用户安全隐私感体验质量进行客观量化评估，具象化产品安全隐私感体验的改进空间，从而推动提升行业整体的安全隐私感设计水平以及用户使用中的安全感。

面向移动互联网产品的用户安全隐私感体验评估实施指南

1 范围

本文件提供了对移动互联网产品的用户安全隐私感体验进行客观有效评估的指导和建议，给出了安全隐私感体验评估指标设计原则、评估指标框架、评估适用场景、评估模型构建方法以及结合具体场景的评估示例等相关信息。

本文件适用于移动互联网产品提供者对其产品开展用户安全隐私感体验方面的自评估，有助于其有针对性地优化设计、提升其产品的安全隐私感体验。

本文件不适用于对物联网、车联网等其他领域的非移动互联网产品进行评估。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动互联网 mobile internet

用户使用移动终端通过移动通信网络获取移动通信网络服务和互联网服务的开放式基础电信网络。移动互联网是移动网和互联网的有机结合。

[来源：YD/T 2960—2015，3.209，有修改]

3.2

安全隐私感 user security and privacy experience

用户在使用移动互联网产品过程中，对其在网络与信息安全、隐私保护等方面的设计方案是否有充足的正向主观感受，主要表现为确定感和控制感两个需求层次。

4 缩略语

下列缩略语适用于本文件。

UI：用户界面（User Interface）

5 移动互联网产品安全隐私感设计模型概述

本文件中，移动互联网产品主要包括在手机、平板等有用户交互界面的移动智能终端上安装和运行的移动应用软件或应用软件的具体功能。移动互联网产品提供者为满足用户在使用中的安全隐私感需求，往往从确定感和控制感两个需求层次构建用户安全隐私感设计模型，其中：

a) 确定感需求：主要是在安全状态下（即客观上不存在威胁且主观上不存在恐惧时）让用户明确的感知到安全保护，在不安全状态下（即客观上存在威胁或用户主观恐惧时）让用户确定知晓如何操作可以恢复到安全状态；

b) 控制感需求：主要是在用户与移动互联网产品的交互过程中，从认知理解到行动操作，再到操作反馈三个阶段，都能确保产品符合用户操作预期和目标。

换言之，确定感是给用户可信赖的主观感受，控制感是给用户可理解、可控制的主观感受。因此，用户安全隐私感设计模型从实现效果及用户期望的目标角度可分为可信赖、可理解、可控制三方面。为了实现上述三方面的效果与目标，需分别制定相应措施，具体包括：

a) 可信赖目标：需从安全保护可感、专业度塑造、安全氛围营造三个维度制定措施；

b) 可理解目标：需从安全策略可理解、界面信息可理解两个维度制定措施；

c) 可控制目标：需从操作透明可预期、预告与反馈两个维度制定措施。

移动互联网产品的用户安全隐私感设计模型见图1。

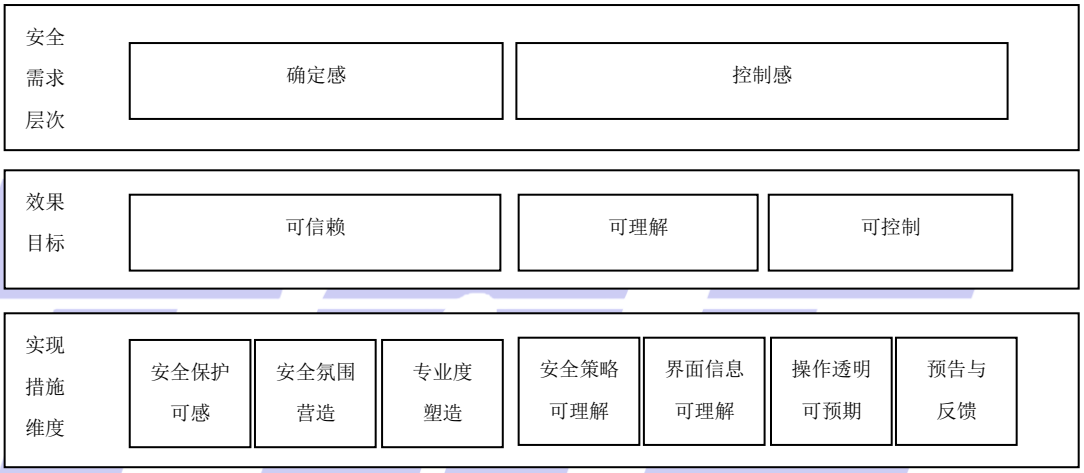


图1　移动互联网产品的用户安全隐私感设计模型

6　安全隐私感体验评估指标设计原则

评估指标是量化评估用户安全隐私感的重要依据，需尽可能从各方面综合反映影响用户安全隐私感的因素。在构建安全隐私感体验评估指标框架时，需考虑以下设计原则：

a) 分层原则：参考心理学研究得出的两个安全需求层次，从确定感和控制感角度进行大颗粒度评估；

b) 细化原则：移动互联网产品基本都涉及用户交互，需针对实现可信赖、可理解、可控制三大目标所采取的每项措施，结合用户设计原则设置细粒度评估指标项，以评估用户的确定感和控制感需求得到满足的程度；

c) 场景化原则：移动互联网产品及功能的使用场景比较多样，需基于以上原则，制定场景化个性化的评估指标值以及相应的计算权重，从而针对性地对每个产品功能的安全隐私感体验进行评估；

d) 可衡量原则：在将主观感知转化为客观水平的过程中，设置的具体指标要符合用户与相关产品技术人员的基本认知，且在可评估；

e) 可实现原则：在设置评价指标值时，要考虑评价数据获取的便利性、可靠性和实际可操作性，以确保最终的评价结果有使用价值和指导意义。

7 安全隐私感体验评估指标框架

7.1 概述

安全隐私感体验评估指标框架可分为两层，第一层宜设置成确定感和控制感两个评估维度，第二层宜结合尼尔森十大交互设计原则及实现可信赖、可理解、可控制三大目标的具体措施设计更具体的细粒度评估指标项。

在设计细粒度评估指标项时，宜优先考虑结合尼尔森十大交互设计原则（见附录A）中适用于构建安全隐私感体验的原则，主要有状态可见原则、环境贴切原则、用户可控原则、容错原则、防错原则、人性化帮助原则。

7.2 确定感指标构成

确定感指标可从用户在安全状态下的感知和不安全状态下的期待两个角度进行评估，宜分为正向显性化感知程度和弱化恐慌性引导程度两个细粒度指标项。

需结合与用户安全隐私感有关的尼尔森交互设计原则以及满足确定感的可信赖目标所对应措施，对确定感的两个细粒度指标项进行细化，具体见表1。

表1 确定感的细粒度指标项细化方式

确定感相关交互设计原则	确定感（可信赖目标）相关措施		
	安全保护可感	专业度塑造	安全氛围营造
状态可见原则	√	√	√
环境贴切原则	—	—	—
用户可控原则	—	—	—
防错原则	—	—	—
容错原则	—	—	—
人性化帮助原则	—	—	√

其中，

a) 正向显性化感知程度指标：宜结合状态可见原则，从安全保护可感、专业度塑造和安全氛围营造方面设计对应的细化指标值：
   1) 安全保护可感：评估安全保护状态可感知可见程度；
   2) 安全氛围营造：评估视觉UI设计专业性、色彩暗示到位程度（如使用蓝、绿色等冷色调）；
   3) 专业度塑造：评估安全认证或权威背书情况呈现强度或用户获知难易度。
b) 弱化恐慌性引导程度指标：宜结合状态可见原则和人性化帮助原则，从安全氛围营造方面设计对应的细化指标值。
   关于安全氛围营造方面，主要评估在可能引发用户恐慌时有无对应的弱化恐慌性引导方案，以及弱化恐慌的力度如何等。

注：例如，有弱化恐慌性引导方案时，评估能否突出如何消除或规避风险、能否有效帮助用户解决当前问题和困惑。

7.3 控制感指标构成

控制感指标可从用户交互的认知、行动、反馈三个阶段进行评估，宜分为安全策略可认知程度、操作可预期可控程度、操作状态反馈有效程度三个细粒度指标项。

需结合与用户安全隐私感有关的尼尔森交互设计原则以及满足控制感的可理解和可控制目标所对应措施，对控制感的三个细粒度指标项进行细化，具体见表2。

表2　控制感的细粒度指标项细化方式

控制感相关交互设计原则	控制感（可理解目标+可控制目标）相关措施			
	安全策略可理解	界面信息可理解	操作透明可预期	预告与反馈
状态可见原则	—	—	√	—
环境贴切原则	√	√	—	—
用户可控原则	—	—	√	—
防错原则	—	—	—	√
容错原则	—	—	—	√
人性化帮助原则	—	—	—	—

其中，

a)　安全策略可认知程度指标：宜结合环境贴切原则，从安全策略、界面信息的用户可理解可接受程度方面设计对应的细化指标值；

注：原则上，需要关注能否避免极其复杂、出乎意料的验证操作，防止出现用户对安全策略不理解或难接受、用户反复尝试才能完成的情况；也需关注是否通过通俗易懂与恰到好处的文案，在敏感页面或核心操作流程中让用户理解。

b)　操作可预期可控程度指标：宜结合状态可见原则、用户可控原则，从操作透明可预期角度设计对应的细化指标值：

1)　状态可见：评估用户是否对操作、流程、反馈的结果可预知，是否不产生用户焦虑；

2)　用户可控：评估操作是否自主可逆，支持撤销、重试。

c)　操作状态反馈有效程度指标：宜结合防错原则和容错原则，从预告与反馈角度设计对应的细化指标值：

1)　防错：评估在关键操作后或状态发生变化时，是否及时提醒用户让其了解所处的状态或规避预防风险；

2)　容错：评估错误信息能否清晰准确地反馈问题所在，是否提供了有效的解决方案。

8　安全隐私感体验评估适用场景

根据用户研究与调研，支付安全、敏感数据保护、纯净体验等是用户重点关注的使用需求。涉及此类功能或场景的移动互联网产品，都需要考虑用户安全隐私感体验方面的评估。

具体适用场景可基于以下原则进行判断：

a)　移动互联网产品的功能存在安全保护机制；

注1：此类场景下，需要关注安全策略是否被有效传达、是否直接可见、是否通俗易懂，操作是否可预期可控制、状态反馈是否及时有效等。

b)　移动互联网产品的功能涉及处理用户的个人隐私。

注2：个人隐私包括但不限于敏感个人信息等，此类场景下，产品设计中往往融入隐私保护设计，需要关注隐私保护设计能否给用户带来足够的正向显性化感知，能否有效减少隐私泄露等可能造成的用户恐慌等。

9　安全隐私感体验评估模型构建方法

在用户使用移动互联网产品的整个旅程中，宜沿着旅程的关键体验节点，结合具体场景对7.2所述的两个确定感的细粒度指标项和7.3所述的三个控制感的细粒度指标项分别设置对应的指标值及计算权重。

针对上述两大评估维度五大指标项的具体指标值及计算权重，可通过专家经验和人因分析（如通过目标用户访谈、调查问券发放、投诉建议反馈等方式收集用户声量并进行分析）进行设计。

移动互联网产品提供者需基于第7章所述的安全隐私感体验评估框架构建评估模型，最终得出评估计算结果（示例详见附录B），具体包括：

a） 根据上述两大评估维度五大指标项的具体指标值及计算权重，对其产品或功能进行逐项评估；

b） 利用每个指标项的实际得分及对应的计算权重得出评估计算结果，可包括安全隐私感整体得分、确定感得分、控制感得分；

c） 通过评估计算结果，得出该产品在确定感、控制感或整体安全隐私感上的体验水平。

注：移动互联网产品提供者还可综合考虑自身、行业或监管情况等因素，对评估计算结果进行分级。

附录C给出了不同场景下，基于本章所述评估模型构建方法针对不同移动互联网产品进行的安全隐私感体验评估示例。

附 录 A
（资料性）
尼尔森十大交互设计原则

哥本哈根人机交互学博士雅各布·尼尔森提出十大交互设计原则，可供移动互联网产品提供者作为启发式方法对其产品的交互设计进行评估，具体包括：

——状态可见原则：在合理时间内给予适当反馈，告知用户正在发生的事情或者当前的状态，减少不确定性，并引导用户正确交互以避免重复操作；

——环境贴切原则：使用目标用户熟悉的语言、单词、短语、图形等，而非晦涩难懂的系统导向术语；遵循现实世界的规律和逻辑来呈现信息；

——用户可控原则：也称撤销重做原则，用户在使用时可能存在误操作或误触某些功能，需要提供明确标识使用户离开该状态，例如取消或撤销功能；

——一致性原则：统一的标准能保证用户更好地理解各设计元素的功能作用，可在设计中建立设计规范文档和可复用组件库，确保同一款产品在功能结构、排版样式、颜色搭配、反馈术语等方面的一致性，减少用户的学习成本；

——防错原则：站在用户角度，预测用户有可能发生错误的操作，尽可能提供相应措施，最大程度减少错误发生，让用户更安心更高效地完成交互；

——易取原则：信息、操作按钮、选项尽量清晰可见，最大程度地减少用户的记忆负担，例如使用说明可见或容易获取等；

——灵活高效原则：需要考虑不同层次或不同类型的目标用户（如新手用户、熟练用户），允许用户根据自己的习惯或需要设置快捷操作或定制常用功能等；

——优美简约原则：页面信息在精而不在多，应突出重点，去除或弱化不相关或不常用信息，让用户更加专注于重要信息；

——容错原则：当用户出现错误时，能够为用户提供清晰易懂且准确的原因描述，并提供有效的解决方案，把用户的损失降到最低；

——人性化帮助原则：最好设计无需提供任何附加提示，但大多时候可能有必要提供简单精准的帮助性提示，例如一次性提示、常驻提示、帮助文档等。

附 录 B
（资料性）
安全隐私感体验评估模型构建举例

指标评估框架如下：

——确定感指标构成：Q={正向显性化感知程度Q1，弱化恐慌性引导程度Q2}；

——控制感指标构成：K={安全策略可认知程度K1，操作可预期可控程度K2，操作状态反馈有效程度K3}。

假设指标值及权重分配如下：

——确定感：总权重为WQ，Q1指标项的指标值总分为SQ1、权重为WQ1，Q2指标项的指标值总分为SQ2、权重为WQ2；

——控制感：总权重为WK，K1指标项的指标值总分为SK1、权重为WK1，K2指标项的指标值总分为SK2、权重为WK2，K3指标项的指标值总分为SK3、权重为WK3。

其中，WQ+WK=1，WQ1+WQ2=1，WK1+WK2+WK3=1。

那么，评估计算结果为：

——确定感得分RQ=WQ*(WQ1*SQ1’+WQ2*SQ2’)，

——控制感得分RK=WK*(WK1*SK1’+WK2*SK2’+WK3*SK3’)，

——安全隐私感整体得分R=RQ+RK。

其中，SQi’（i=1,2）、SKj’（j=1,2,3）是某项移动互联网产品分别在确定感、控制感的每个指标项上的实际得分。

综上，可通过对比确定感得分及其总分情况，或者对比控制感得分及其总分情况，分析该产品在确定感或控制感上的设计水平。同样地，可通过对比整体得分及其总分情况，分析该产品的整体安全隐私感体验水平。

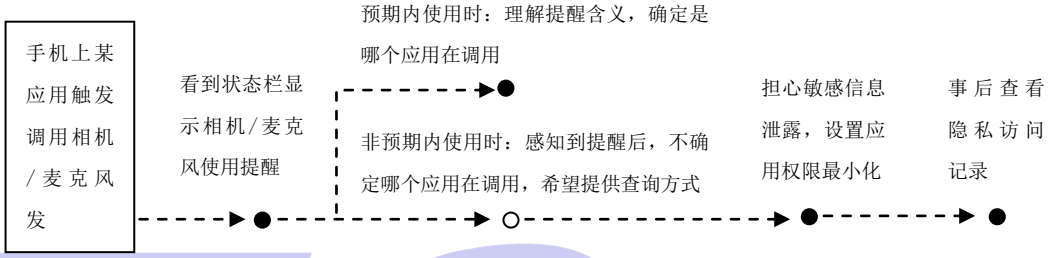
附 录 C
（资料性）
结合具体场景的评估示例

C.1 终端敏感权限使用状态提醒功能场景下的评估示例

下面以终端敏感权限使用状态提醒功能场景为例。

a) 场景描述：用户在正常使用手机过程中，手机上某应用触发调用相机或麦克风权限后，敏感权限使用状态提醒功能开始工作。

b) 用户使用旅程：用户旅程中的关键体验节点见图C.1。



图C.1 用户旅程中的关键体验节点

沿着旅程的关键体验节点，明确评估用户安全隐私感的细粒度指标项：

1) 针对用户看到状态栏显示相机/麦克风使用提醒节点，设计两个评估指标项：
   - 确定感_正向显性化感知程度：相机/麦克风被使用的实时显性提醒，让用户感知哪个权限正被调用；
   - 控制感_安全策略可认知程度：相机/麦克风使用提醒的方式合理、直观、易理解。

2) 针对用户是否可预期节点，设计两个评估指标项：
   - 确定感_弱化恐慌性引导程度：显性引导如何查看哪个应用在调用相机/麦克风权限、能否修改权限的授予状态，避免用户恐慌；
   - 控制感_操作可预期可控程度：允许直接点击提醒，查看应用信息以确认是否符合预期。

3) 针对用户设置应用权限节点，设计一个评估指标项：
   - 控制感_操作可预期可控程度：允许一步跳转到权限控制页面，可关闭不符合用户预期的应用使用该敏感权限。

4) 针对用户事后查看隐私访问记录节点，设计一个评估指标项：
   - 控制感_操作状态反馈有效程度：提供各应用使用敏感权限记录，方便用户在感知到发生敏感权限被调用后能通过使用记录查看与核对。

c) 设计评估用例：

利用人因分析（包括目标用户访谈、用户实际使用情况分析等方式）和专家经验方法，得出每个细粒度指标项对应的指标值及计算权重，见表C.1：

表C.1　该场景下评估指标项的指标值及权重设计、评估得分计算示例

评估维度 （一级指标）	指标项 （二级指标）	指标值 （SQi=5, i=1, 2；SKj=5, j=1, 2, 3）	实际得分
确定感 （WQ：50%）	1、确定感_正向显性化感知程度 （WQ1:40%）	1. 相机/麦克风被使用时给用户提醒（1分） 2. 相机/麦克风被使用中通过显性标识实时持续提醒（2分） 3. 提醒标识采用冷色调显示系统正在实时守护用户，给用户安全感（1分） 4. 提供用户设置相机/麦克风使用提醒的途径（1分）	SQ1’
	2、确定感_弱化恐慌性引导程度 （WQ2:60%）	1. 提供引导查看使用相机/麦克风的应用信息（3分） 2. 提供引导设置应用使用相机/麦克风的权限（2分）	SQ2’
控制感 （WK：50%）	3、控制感_安全策略可认知程度 （WK1:20%）	1. 有提醒标识，如通用标识（2分） 2. 提醒标识可解释，如首次展示通用标识时提供相应文案解释含义，或展示过程中通过图形变换解释标识含义（调用时短暂展示麦克风图案后迅速变成通用标识）（2分） 3. 提醒标识持续定制化提醒，如显示相机图标/麦克风图标（1分）	SK1’
	4、控制感_操作可预期可控程度 （WK2:60%）	1. 用户可在两步及以内操作查看到使用相机/麦克风的应用信息（1分） 2. 用户可一步操作查询具体访问相机/麦克风的应用信息（如下拉状态栏）（1分） 3. 用户无需学习即可操作查询访问相机/麦克风的应用信息（如直接点击提醒）（1分） 4. 可以一步跳转权限控制，关闭应用被授予的相机/麦克风权限（2分）	SK2’
	5、控制感_操作状态反馈有效程度 （WK3:20%）	1. 各应用敏感权限使用情况有记录反馈可供查看（3分） 2. 系统反馈的敏感权限使用记录与用户通过提醒标识查询到的应用信息一致（2分）	SK3’
计算方法： 1）　各二级指标项实际得分SQi’/SKj’ = 各指标值对应得分的叠加，再乘以对应二级权重WQi/WKj； 2）　一级指标实际得分RQ/RK = 各二级指标项实际得分的叠加，再乘以对应一级权重WQ/WK； 3）　总分R = 各一级指标实际得分的叠加。			

d）　评估结论举例：

用户在使用该功能时，相机/麦克风被调用后在主页面有特殊提醒标识，但标识含义未直接凸显被调用对象（即标识定制化尚缺失）；用户想查看/设置正在调用相机/麦克风权限的应用时，需要两步操作实现（即一步操作或无需学习即可操作方式尚未实现）。

按上述评估模型，最终评估结果为：

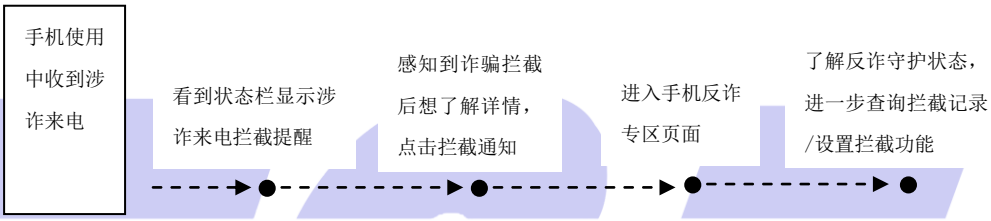
1) 确定感得分：50%*(40%*5+60%*5)=2.5分(该项满分2.5分)，表现很好；
2) 控制感得分：50%*(20%*4+60%*3+20%*5)=1.8分(该项满分2.5分)，控制感一般，需减少操作交互复杂度提升用户控制感；
3) 整体得分：4.3分(满分5分)。

通过评估得出，该产品功能的整体安全隐私感良好，其中确定感很好、控制感一般。该产品的安全隐私感设计可在操作交互复杂度方面进行优化。

C.2 电信网络涉诈检测预警场景下的评估示例

下面以电信网络涉诈检测预警场景为例。

a) 场景描述：用户在正常使用手机过程中，接打涉诈电话、收发涉诈短信、安装涉诈应用时，涉诈检测预警功能开始工作。
b) 用户使用旅程：以收到涉诈来电为例，用户旅程中的关键体验节点见图C.2。



图C.2 用户使用旅程中的关键体验节点

沿着旅程的关键体验节点，明确评估用户安全隐私感的细粒度指标项：

1) 针对用户看到涉诈来电拦截提醒节点，设计两个评估指标项：
   - 确定感_正向显性化感知程度：诈骗可能发生时显性呈现拦截标识，设置反诈专区集中展示防护能力；
   - 确定感_弱化恐慌性引导程度：给出涉诈预警的同时，提供消除风险措施或建议。
2) 针对用户主动了解拦截详情节点，设计一个评估指标项：
   - 控制感_安全策略可认知程度：诈骗拦截通知内容直观、易理解，如使用盾牌/阻断标识/简单易懂的文字说明。
3) 针对用户在反诈专区查看反诈守护详情节点，设计四个评估指标项：
   - 确定感_弱化恐慌性引导程度：引导用户设置反诈相关功能，预防诈骗发生；
   - 控制感_安全策略可认知程度：反诈功能使用描述直观、易理解，工作逻辑描述合理；
   - 控制感_操作可预期可控程度：允许用户查看诈骗拦截记录，允许用户设置自主管控涉诈应用；
   - 控制感_操作状态反馈有效程度：用户执行高风险操作时（如关闭反诈功能、移除黑名单等），提醒谨慎操作或要求二次确认。

c) 设计评估用例：

利用人因分析（包括用户实际使用情况分析、特定群体用户访谈、执法案例调研、监管要求等方式）和专家经验方法，得出每个细粒度指标项对应的指标值及计算权重，见表C.2。

表C.2　该场景下评估指标项的指标值及权重设计、评估得分计算示例

评估维度 （一级指标）	指标项 （二级指标）	指标值 （SQi=5, i=1, 2；SKj=5, j=1, 2, 3）	实际得分
确定感 （WQ：70%）	1、确定感_正向显性化感知程度 （WQ1:50%）	1. 有显性涉诈拦截标识，如状态栏/弹框提醒等（1分） 2. 有反诈专区呈现拦截记录（1分） 3. 反诈专区提供功能集中设置入口，增加用户确定感（1分） 4. 反诈专区通过色调营造安全守护氛围（无涉诈风险时使用冷色调提示用户处于安全状态；有涉诈风险中使用暖色调警示）（1分） 5. 反诈专区体现权威数据来源或认证情况（1分）	SQ1’
	2、确定感_弱化恐慌性引导程度 （WQ2:50%）	1. 接打涉诈电话时提醒风险并引导消除风险的操作（1分） 2. 收发涉诈短信时提醒风险并引导消除风险的操作（1分） 3. 安装诈骗应用时提醒风险并引导消除风险的操作（1分） 4. 有涉诈风险的行为（共享屏幕/转账等），提醒风险并引导消除风险的操作（1分） 5. 反诈功能未开启时引导用户开启相关功能，预防诈骗风险（1分）	SQ2’
控制感 （WK：30%）	3、控制感_安全策略可认知程度 （WK1:20%）	1. 诈骗电话/短信的拦截提示使用通用标识（1分） 2. 诈骗电话/短信的拦截提示标识更直观、易理解，或使用定制化标识（1分） 3. 发生涉诈风险时的界面提示信息和二次确认方式易理解（2分） 4. 反诈功能简述直观、易理解（1分）	SK1’
	4、控制感_操作可预期可控程度 （WK2:50%）	1. 用户在反诈专区查询拦截记录时可以呈现详细相关信息，如：时间/电话号码/短信内容/应用名等（2分） 2. 用户在反诈专区设置相关功能（如拦截规则、阻断功能等）后可按用户自定义方式相应拦截（2分） 3. 用户可在反诈专区上报/共享涉诈资源，如电话、应用等（1分）	SK2’
	5、控制感_操作状态反馈有效程度 （WK3:30%）	1. 关闭反诈相关功能时，提醒谨慎操作（1分） 2. 关闭每项涉诈风险检测功能时，都会提醒谨慎操作（2分） 3. 移除被管控对象（如号码、应用黑名单）时，给用户二次提醒（2分）	SK3’
计算方法： 1）　各二级指标项实际得分SQi’/SKj’ = 各指标值对应得分的叠加，再乘以对应二级权重WQi/WKj； 2）　一级指标实际得分RQ/RK = 各二级指标项实际得分的叠加，再乘以对应一级权重WQ/WK； 3）　总分R = 各一级指标实际得分的叠加。			

d) 评估结论举例：

用户使用手机中该功能开始工作时，在状态栏有涉诈拦截标识，也有反诈专区呈现拦截记录以及提供功能设置入口，但未呈现相关权威依据说明（如数据来源或权威认证）；该功能提供的反诈专区可呈现详细的拦截记录，允许用户自由开关或设置拦截规则，但关闭单项反诈功能时未做二次提醒、尚无统一的用户上报入口。

按上述评估模型，最终评估结果为：

1) 确定感得分：70%*(50%*4+50%*4)=2.8分(该项满分3.5分)，表现良好，但外部权威认证说明或引入、风险消减引导措施仍需加强；
2) 控制感得分：30%*(20%*4+50%*4+30%*3)=1.11分(该项满分1.5分)，表现一般，可在用户主动上报风险、关闭反诈功能的二次提醒方面增加需求；
3) 整体得分：3.91分(满分5分)。

通过评估得出，该产品功能的整体安全隐私感较好，其中确定感良好、控制感一般。该产品的安全隐私感设计可在外部权威认证说明或引入、风险消减引导措施、增加用户主动上报风险及关闭反诈功能时的二次提醒等方面进行优化。

参 考 文 献

[1] YD/T 2960—2015 移动互联网术语

[2] 安莉娟,丛中.安全感研究述评[J].中国行为医学科学,2003,12(6):698-699.

[3] OPPO.2021 年中国智能手机用户安全需求洞察报告.2021.

[4] 吴彩虹.移动支付中的安全交互体验设计研究[D].上海:上海交通大学,2015.

[5] 王俊秀,刘洋洋.中国居民隐私安全感的变化及其影响因素——基于年龄-时期-队列分析[J].江苏行政学院学报,2021(6):67-76.

[6] 于世刚.确定感、安全感、控制感——人的安全需要的三个层次[J].社会心理科学,2011,26(2):3-8.

[7] 张勉.智慧城市建设的市民安全感评价和提升研究[D].东南大学,2022.

[8] OIMIL. 从安全需求的三个层次，提高用户的安全感.https://www.woshipm.com/pd/666135.html

[9] 知乎.移动互联网用户感知评估体系研究.https://zhuanlan.zhihu.com/p/148587336

电信终端产业协会团体标准

面向移动互联网产品的用户安全隐私感体验评估实施指南

T/TAF 226—2024

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn