ICS 35.040
CCS L 80

团　体　标　准

T/TAF 142—2022

eUICC卡生产企业安全保障能力要求

Security requirements for embedded UICC manufacturing enterprise

2022-12-29 发布　　2022-12-29 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：中国信息通信研究院、中国电信股份有限公司、中国移动通信集团有限公司、中国联合网络通信有限公司、泰尔认证中心有限公司、博鼎实华（北京）技术有限公司、恒宝股份有限公司、恩智浦（中国）管理有限公司、武汉天喻信息产业股份有限公司、紫光同芯微电子有限公司、北京中电华大电子设计有限责任公司、东信和平科技股份有限公司。

本文件主要起草人：薛刚、胡越男、李杰强、李俊宏、陈思宇、武小芳、郑海霞、崇静、张知晓、卢丽敏、张苒、徐从德、刘扬、贾翔榆、黄健文、周江、梁宇、朱在鹏、张一成、魏鑫宇、谢懿、刘嘉维、孙亨博、张娟娟、郑士超。

引　　言

近年来，随着《中华人民共和国网络安全法》和《中华人民共和国数据安全法》等法律的实施，对相关企业和产品的安全要求日益提高。eUICC卡产品的生产过程涉及个性化的数据，面临较大的安全风险，因此生产企业的安全保障能力至关重要。

本文件面向eUICC卡生产企业，提供一套安全保障体系框架和基本的安全保障能力要求，可促进企业提高自身安全管理水平、对满足国家法律法规要求和监管部门合规要求也具有积极的作用。

eUICC卡生产企业安全保障能力要求

1 范围

本文件规定了eUICC卡生产企业的安全保障能力要求，包括安全保障体系框架、安全保障体系和具体的安全保障能力要求。

本文件适用于eUICC卡生产企业改进自身安全管理水平。需要时，也可以作为eUICC卡的采购方和第三方机构对eUICC卡生产企业进行安全性评价的依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。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。

ISO/IEC 27000 信息技术 安全技术 信息安全管理体系 概述和词汇（Information technology-Security techniques-Information security management systems-Overview and vocabulary）

3 术语和定义

下列术语和定义适用于本文件。

3.1

eUICC卡个人化生产企业 eUICC personalisation manufacturing enterprise

实施eUICC卡个人化生产的组织。

注：本文件中如未特殊指明，以“eUICC卡生产企业”指代“eUICC卡个人化生产企业”。

3.2

eUICC卡个人化生产 eUICC personalisation manufacturing

将eUICC卡相关证书信息、密钥或其他必要的相关敏感数据写入eUICC卡中的生产过程。

4 安全保障体系

4.1 安全保障体系框架

a) 安全保障体系框架见图A.1；

b) 组织的战略需考虑安全发展要求，识别内外部环境的变化，并明确与战略匹配的安全保障需求。通过持续打造安全保障能力，获得期望的安全保障，实现战略落地。通过对战略循环过程进行跟踪评测，寻求战略、安全保障需求和安全保障能力互相匹配且不断改进的机会；

c) 组织应根据本文件第5部分的要求及组织确定的安全能力要求，通过发挥人员、设备、网络、环境、过程和数据的协同作用，实现数据在生产过程的持续安全；

d) 组织应围绕人员、设备、网络、环境、过程和数据的要求，充分发挥领导的核心作用，建立策划、支持、实施与运行、评测与改进管理机制，规范安全管理，推动安全保障能力的持续提升，稳定获取期望的安全保障。

4.2 安全保障体系

4.2.1 总则

组织应充分认识影响其安全发展的内外部环境变化，按照本文件的要求，建立、实施、保持和改进安全保障体系，以持续打造并保持安全保障能力，获取与组织战略相匹配的安全保障。

4.2.2 识别组织的内外部环境

组织应识别与安全保障有关的各种外部和内部因素。

组织应对这些外部和内部因素的相关信息进行分析和确定。

注1：外部因素包括政策、法律法规要求、相关方的需求和期望、本文件的要求。

注2：内部因素包括组织内部的文化、方针和现状等。

4.2.3 获得安全保障

组织应根据其战略，结合内外部环境的变化，对安全保障需求进行识别、调整、评审和确定。

组织应按照确定的安全保障需求，对安全保障能力进行策划、实施、运行、评测和改进，确保获得与组织战略相匹配的安全保障。

组织的安全保障能力至少应满足本文件第5部分的要求。

4.2.4 安全保障体系的变更

当组织需要对安全保障体系进行变更时，应考虑：

a) 变更目的及其潜在后果；

b) 安全保障体系的连续性和完整性；

c) 资源的可获得性；

d) 人员职责和权限的分配或再分配。

4.2.5 文件化信息

安全保障体系文件化信息包括：

a) eUICC卡个人化生产的范围和边界；

b) 安全保障需求；

c) 安全保障能力要求；

d) 组织确定的为确保安全保障体系有效性所需的文件化信息。

4.2.6 领导作用

组织的管理层应通过以下活动，证实对安全保障体系的领导和承诺：

a) 确保建立至少满足本文件第5部分要求的安全保障能力；

b) 将安全保障体系要求整合到组织的过程中；

c) 确保安全保障体系需要的资源；

d) 确保与安全保障有关的责任和权限得到分配与沟通；

e） 确保安全保障体系达到预期结果；
f） 促进持续改进。

4.2.7 策划

组织应围绕安全保障需求，按照形成的规定及本文件第5部分的要求，对安全保障能力进行识别、调整、评审和确定，并保留文件化信息。

4.2.8 支持

组织应确定并提供安全保障体系所需的内外部资源、围绕实现安全保障能力进行统筹配置，包括资金、人员、设备、网络和环境等。

4.2.9 实施与运行

a） 组织应按照在策划中确定的安全保障能力制定相应的实施方案，并推动方案落地和运行，以打造并保持安全保障能力；
b） 组织应主动管理实施与运行过程，推动人员、设备、网络、环境、过程和数据的协同优化。

4.2.10 评测

a） 组织应对安全保障体系进行评测，以判断其有效性；
b） 组织应确定评测的时间、内容和方法。

4.2.11 改进

a） 组织应对发现的不符合情况进行纠正，并分析不符合的原因并采取措施防止再次发生；
b） 组织应持续改进安全保障体系的适宜性、充分性和有效性。

5 安全保障能力要求

5.1 人员要求

a） 组织应分配独立的人员（必要时设置独立的机构）负责安全问题的识别、确认、协调和解决。人员或机构应具备相应的能力和职权，并应与业务部门相互独立。人员或机构的职责和权限应在文件中做出明确规定；
b） 组织应与所有人员签署保密协议；
c） 组织应制定安全准则和指南，必要时应对员工进行培训，以便员工理解并遵守组织的安全要求。对于违反安全准则的人员，应按照规定进行处理；
d） 对于离职人员，应制定充分且适宜的离职程序，防止人员离职引发的安全风险。

5.2 设备要求

a） 组织应对生产设备、检测设备及配套设备制定适宜的管理程序，对设备的管理、采购、使用、维护、检测和淘汰做出明确的规定；
b） 组织配备的生产设备和检测设备应来源可靠，且在受控状态下才允许被访问和使用，以确保数据安全；
c） 必要时，组织应对生产和检验人员进行培训和考核，确保其具备相应的能力。

5.3 网络要求

a） 组织应对网络的访问、使用、运行、维护和安防制定适宜的管理程序；
b） 组织应将与生产相关的网络与其他网络进行隔离；
c） 组织应配备适当的网络安全产品来降低网络风险；
d） 对于生产网络的访问应进行严格的限制，当进行远程访问时，应建立更严格的授权和验证机制；
e） 组织应以适当的频率对网络进行风险排查，以持续维护网络安全。

5.4 环境要求

a） 组织应具备用于生产、检验和存储产品的安全场所；
b） 安全场所应具有充足的安全防护措施，确保能抵挡适当时间的物理侵入；
c） 安全场所应具有访问控制措施，确保能阻止非法访问；
d） 安全场所应配备适当的安防设备和安保人员；
e） 适用时，安全场所应满足静电防护要求。

5.5 过程要求

a） 产品的原材料获取应在受控状态下进行，确保原材料满足生产需求和安全要求；
b） eUICC证书的生成和签署应该在受控状态下进行，且事后可追溯；
c） 产品的生产过程应在受控状态下进行，应能查看生产过程参数和结果参数；
d） 产品的检验过程应在受控状态下进行，应能查看检验过程参数和结果参数；
e） 产品的交付过程应在受控状态下进行，确保交付产品的安全性和一致性；
f） 不合格产品的处置过程应在受控状态下进行，确保不合格产品不会造成安全风险。

5.6 数据要求

a） 组织应对数据进行分类并确定敏感程度，并按照数据的敏感程度制定不同的保护策略和措施。这些措施应形成文件化的规定，并通过分发、培训和考核使相关员工充分理解并实施；
b） 组织应将eUICC证书和密钥确定为高敏感数据；
c） 对敏感数据的保护措施应覆盖数据创建、存储、传输、使用和销毁的全过程和人员、设备、网络、环境、过程的全维度；
d） 对敏感数据的访问和使用应受到严格的限制，只在必要的情况下经审批和授权后才可以进行，且事后可追溯。

附 录 A
（资料性）
eUICC卡生产企业安全保障体系框架

eUICC卡生产企业安全保障体系框架见图A.1。

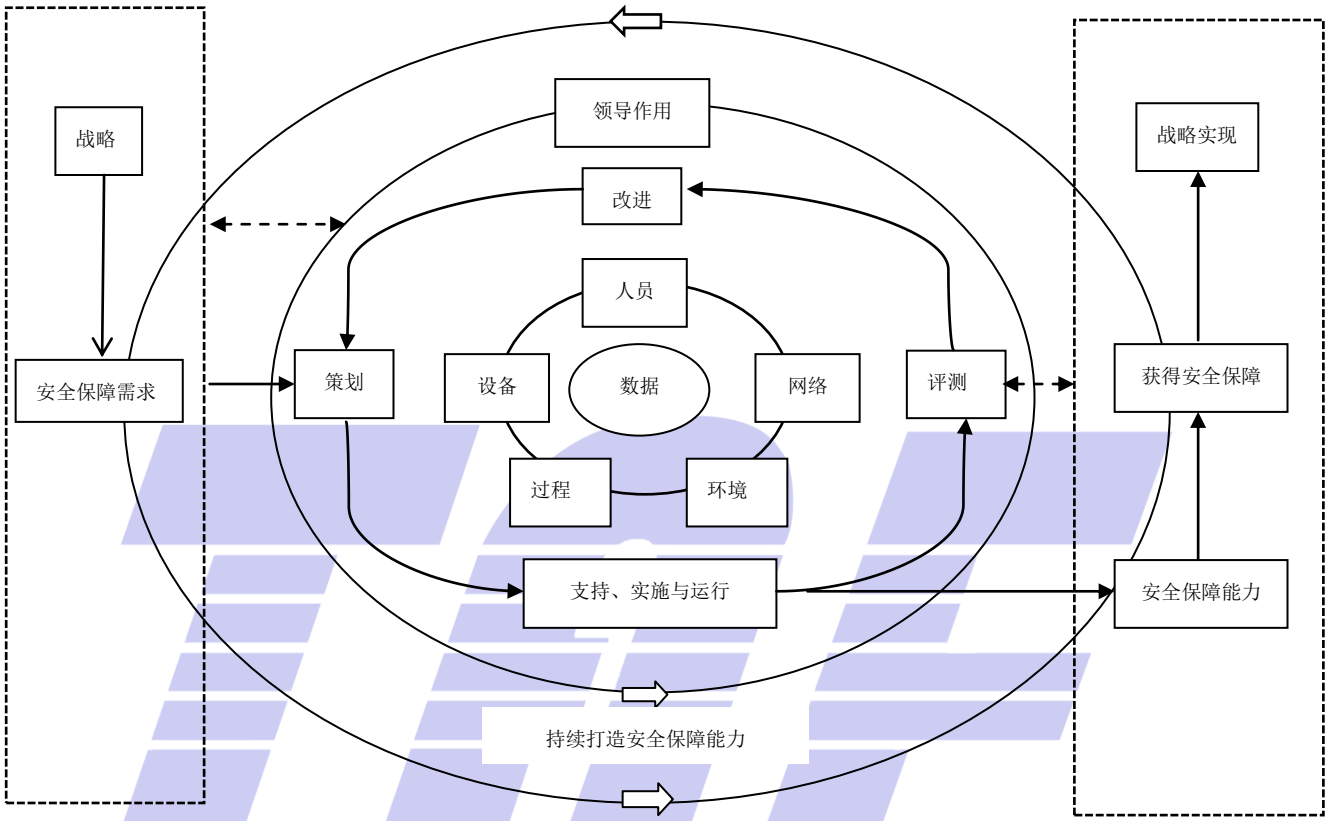

图 A.1 eUICC 卡生产企业安全保障体系框架

电信终端产业协会团体标准

eUICC卡生产企业安全保障能力要求

T/TAF 142—2022

*

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