ICS 35.240
CCS L67

团　　体　　标　　准

T/CCSA XXXX—XXXX
[代替 T/CCSA]

面向供应链的信息技术产品通用安全能力要求

Information technology product security capability requirements for supply chain

（报批稿）

2025.07.16

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国通信标准化协会　发　布

目　　次

前　　言.....II
引　　言.....III
1 范围.....4
2 规范性引用文件.....4
3 术语和定义.....4
4 缩略语.....4
5 总体说明.....5
6 安全功能要求.....5
7 安全保障要求.....7

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》的规则起草。

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这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、中国电信集团有限公司、中国移动通信集团有限公司、中兴通讯股份有限公司、蚂蚁科技集团股份有限公司、浪潮电子信息产业股份有限公司、北京安普诺信息技术有限公司、北京天融信网络安全技术有限公司、杭州默安科技有限公司

本文件主要起草人：

引　言

面向供应链的信息技术产品通用安全能力要求

1 范围

本文件规定了供应链场景下信息技术产品安全能力要求，从安全功能要求、安全保障要求两大维度，围绕访问通道控制、应用安全、加密要求、敏感数据保护、产品系统安全管理、产品完整性校验、安全资料、用户隐私保护、安全开发交付要求、系统加固、生命周期支持等重点内容进行要求规范。

本文件适用于供应链场景下为供应商信息技术产品安全基线的设计、开发和检验提供指导，同时也可为第三方机构对于产品安全能力要求进行审查和评估时提供依据。

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。

GB/T 11457-2006 信息技术　　软件工程术语

GB/T 32921-2016 信息安全技术 信息技术产品供应方行为安全准则

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息技术产品 information technology product

具有采集、存储、处理、传输、控制、交换、显示数据或信息功能的硬件、软件、系统和服务。

注：信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

[来源：GB/T 32921-2016，定义3.1]

3.2

软件 software

与计算机系统的操作有关的计算机程序、规程和可能相关的文档。

[来源：GB/T 11457-2006，定义2.1469]

4 缩略语

下列缩略语适用于本文件。

IP：互联网协议（Internet Protocol）
LAN：局域网（Local Area Network）
WAN：广域网（Wide Area Network）

5 总体说明

5.1 安全能力要求分类

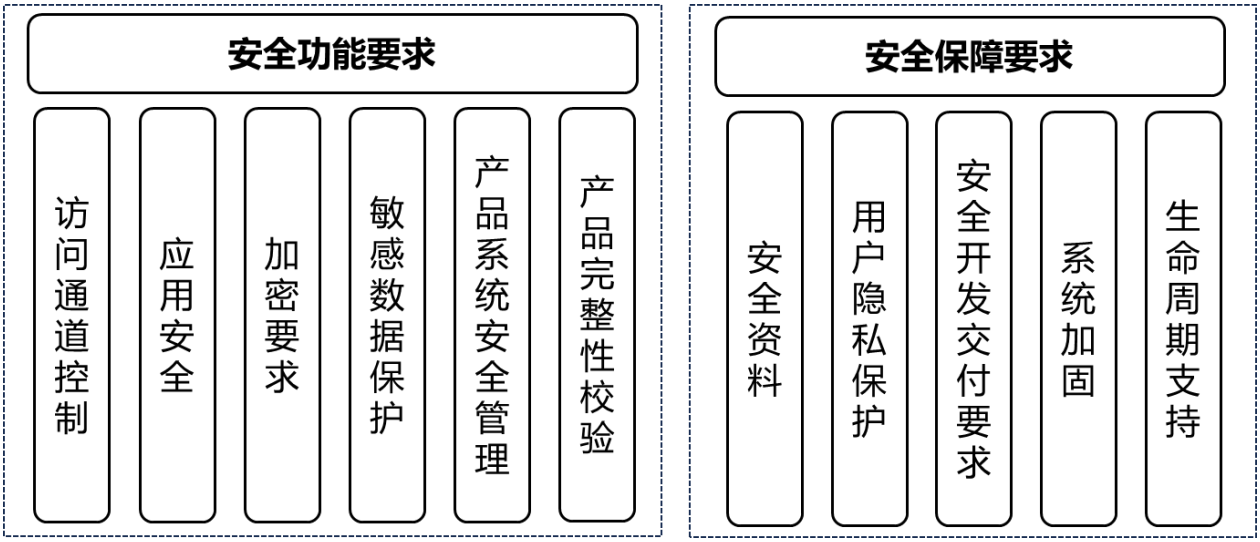

图1 面向供应链的信息技术产品通用安全能力要求框图

6 安全功能要求

6.1 访问通道控制

访问通道控制指信息技术产品供应商通过网络隔离等手段，减少攻击面，降低产品被攻击的风险。具体要求包括但不限于：

——针对支持独立管理IP地址的产品，系统应支持无法从用户面直接登陆连接管理接口；

——产品系统对外通信连接应是系统运行和维护必需的，应通过端口扫描工具验证，将未在通信矩阵中列出的端口进行关闭；

——针对同时存在跨公网和局域网的产品，面向公网的WAN侧管理端口和面向局域网LAN侧管理端口应隔离管理；

——应用界面与管理界面应隔离管理；

——除标准协议不具备认证机制外，对系统进行管理的接口应支持接入认证机制；

——针对产品外部可见的，能对系统进行管理的物理接口应支持接入认证机制。

6.2 应用安全

应用安全指信息技术产品供应商应通过技术手段，降低应用安全风险。具体要求包括但不限于：

——产品应支持对于需要访问授权的请求进行用户权限核实，明确授权操作；

——产品对用户权限的最终认证鉴权过程应在服务端进行；

——针对产品Web应用程序的会话标识应具备随机性，用户身份验证成功后，应更换会话标识；

——产品应支持在服务器端对来自不可信数据源的数据进行校验，拒绝没有通过校验的数据。

6.3 加密要求

加密要求指产品使用的加密算法满足安全要求。具体要求包括但不限于：

——产品应使用已标准化的密码算法，包括但不限于国际标准、国家标准或行业标准等已标准化的密码算法；

——产品使用的密码算法库应通过认证机构认证、业界开源公认或经企业内部评估认可；

——密码算法中使用到的随机数必须是密码学意义上的安全随机数；

——产品在初始安装应默认使用安全算法，升级场景可保持兼容，并提示用户风险；

——产品代码中用于数据加解密的工作密钥应加密处理，根密钥场景可对部分密钥组件进行硬编码处理。

6.4 敏感数据保护

敏感数据保护指产品对敏感数据的存储、传输和处理应保证数据安全，防止数据泄露。具体要求包括但不限于：

——认证凭据应加密存储在产品系统中，针对不需要还原明文的场景，应使用不可逆加密算法；

——在非信任网络之间进行敏感数据的传输须采用安全传输通道或者加密后传输；

——对敏感数据的访问应具备认证、授权、或加密机制；

——在系统存储的日志、调试信息、错误提示中应禁止打印认证凭据等敏感数据；

——在设备维修、销毁的场景下，需提供安全删除数据（含个人数据、客户数据等）的能力；

——系统中所采集、使用的敏感数据应遵循最小化原则。

6.5 产品系统安全管理

产品系统安全管理明确产品系统安全模块应具有的功能，保证系统自身账号口令、配置的安全管理。具体要求包括但不限于：

——产品自身的口令应满足常见安全要求，包括但不限于口令长度、口令复杂度；

——产品认证模块应支持口令防暴力破解机制，当重复输入错误口令次数超阈值时应采取相应保护措施，包括但不限于锁定账号、锁定IP、延迟登录、验证码、IP白名单等；

——操作界面的口令不应直接明文显示；

——操作界面口令输入框内容应禁止拷贝；

——针对产品的口令密文应设置访问控制；

——对系统产生影响的用户活动、操作指令等应纳入记录日志并统一管理，记录日志内容应详尽完善，支持事后审计；

——针对记录日志应设置访问控制，同时禁止提供手动删除、修改记录日志的能力；

——产品系统的管理平面和近端维护终端、网管维护终端间，应默认使用安全传输协议；

——产品外部可访问的所有账号的缺省口令应在系统初始设置时强制修改，且口令满足口令复杂度要求；

——产品正常运行后，管理员新建/重置账号应设置初始口令或系统自动产生随机口令，且口令满足口令复杂度要求；

——系统应有明确的用户权限管理机制，新建账号默认不授予任何权限或者默认只指派最小权限的角色。

6.6 产品完整性校验

产品完整性校验指对外发布的产品自身具有完整性校验机制，防止产品被攻击者恶意篡改。具体要求包括但不限于：

——产品对外发布的软件（包含软件包/补丁包）应提供完整性校验机制，在安装、升级过程中自动进行完整性验证；

——重点场景的信息技术类产品应支持安全启动。

7 安全保障要求

7.1 安全资料

安全资料指对针对对外提供的产品应配套安全方案、资料，说明必要安全信息和安全使用方式。具体要求包括但不限于：

——产品发布的安全资料中应提供产品通信矩阵，描述机器/网元/模块间的通信关系，内容包括但不限于：通信使用的端口、协议、IP地址、认证方式、端口用途信息等；

——产品系统对使用到的通信端口应在产品通信矩阵文档中说明；

——产品发布的安全资料中应提供安全配置/加固指南（产品、开源和第三件的使用）；

——产品发布的安全资料中应提供产品缺省内置的账号清单。

7.2 用户隐私保护

用户隐私保护指产品对个人数据的采集、传输、处理、存储遵循相关法律法规要求，并提供必要的隐私声明和保护机制。具体要求包括但不限于：

——产品应在资料中提供产品处理的个人数据说明，并对产品涉及用户隐私的功能进行描述；

——收集或使用个人数据前，应明确提示用户，并获得用户的同意，并且允许用户随时关闭对个人数据的收集和使用；

——产品仅收集业务处理所必须的个人数据，且收集处理个人数据的范围、目的应与隐私声明或个人数据说明保持一致；

——对个人数据采集或处理的相关操作，产品应提供安全保护机制（如认证、权限控制、日志记录等），防止个人数据被泄漏；

——产品从用户网络传出数据，应具备对其中的个人数据进行过滤、或匿名化处理的能力，确保不能以任何方式还原个人数据；

——正常业务流程或标准协议允许的情况下，允许提供用户精确位置定位的功能，其他场景禁止提供用户精确位置定位的功能；

——对系统或软件进行升级时应通过界面或者资料的形式让用户知情且可控；

——产品应提供个人数据删除或匿名化处理的能力。

7.3 安全开发交付要求

安全开发要求指产品设计、编码、编译等符合安全要求，降低安全风险。具体要求包括但不限于：

——产品自研代码应经过静态应用程序安全测试工具扫描，并按照工具相应风险提示进行风险处理；

——产品自研代码应按照相应的编程规范使用安全函数替换不安全函数，不应使用不正确的重定义安全函数或不正确的封装安全函数；

——产品开源代码应从可信数据源获取，获取源头包括但不限于：开源软件官网、国内外主流代码托管平台、开源基金会；

——产品开发过程应按规范开启安全编译选项；
——产品中应不存在可绕过系统安全机制，如认证、权限控制、日志记录等，对系统或数据进行访问的功能；
——产品应经过检验检测，不存在已知的病毒、木马等；
——产品应经过检验检测，不存在发送恶意广告、吸费、恶意消耗流量等的行为；
——产品应经过检验检测，不存在存疑的组件，包括但不限于第三方的网络嗅探、调试工具、开发/编译工具、在调测阶段使用的认证密钥、自研调试工具/脚本等；
——产品应经过检验检测，不存在用户界面不可见或产品资料未描述的未公开的公网地址，包括但不限于公网IP地址、公网URL地址/域名、邮箱地址等；
——产品应经过检验检测，不存在破坏OS等系统原有安全框架，被外界质疑为后门的行为；
——产品应经过检验检测，不存在对外提供服务和能够被远程访问的进程使用root账户（或等同）权限运行。

7.4 系统加固

系统加固指产品应采取安全措施，保证产品自身和运行环境的安全。具体要求包括但不限于：
——产品系统应经漏洞扫描工具扫描，评估漏洞风险级别，高风险级别的漏洞应得到解决或有效规避；
——产品应梳理使用的开源或第三方软件等存在的外部公开漏洞，已有官方修复方案的，应按照官方认可的方案进行修复；
——产品应经过检验检测，对公网开放的服务不包括高危服务，包括但不限于使用不安全协议的服务、存在高危漏洞的服务。

7.5 生命周期支持

生命周期支持指针对发布的产品，提供支持保障产品在生命周期内得到持续安全更新。具体要求包括但不限于：
——产品所使用的平台版本组件、开源和第三方件软件禁止使用停止维护的版本；
——应梳理所使用到的开源及第三方软件信息，明确使用版本，并输出开源及第三方软件清单；
——应针对产品形成软件物料清单清单，明确产品组成信息和依赖关系；
——应针对产品建立全生命周期监控机制，发现产品漏洞应按照漏洞处理标准及时上报并修复。