ICS 35.020
I651

T/ SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/SIA 008.2—2018

就绪可用软件产品（RUSP）安全质量评价标准 第 2 部分　安全质量要求和等级划分指南

Ready to Use Software Product (RUSP) Security Evaluation Criteria—Part 2：Security Quality Requirements and Grading Guideline

2018-12-12 发布　　2018-12-12 实施

中 国 软 件 行 业 协 会　发 布

目　录

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准的本部分由中国软件行业协会提出并归口。

本标准的本部分主要起草单位：中国软件行业协会系统安全工程分会、大连理工大学、北京天融信网络安全技术有限公司、联想集团（北京公司）、远光软件股份有限公司、北京圣世信通科技发展有限公司。

本标准的本部分主要起草人：宋明秋、付晓宇、陈宝国、张然、陈兴跃、李汝鑫、李锋、李广志。

本标准的本部分为首次制定。

1 范围

本标准的本部分定义了：

a）就绪可用软件产品（RUSP）的安全质量要求和质量等级划分原则。

b）本部分为就绪可用软件产品（RUSP）安全质量评价标准的第2部分。

c）本部分在GB/T 25000.51/ISO/IEC 25051的软件质量要求，以及T/SIA 008.1-2018软件安全质量模型基础之上，结合信息技术安全评估准则（GB/T 18336.2 、GB/T 18336.3）、等级保护测评要求（GB/T 28448-2012）和“代码安全审计规范”，进一步清晰阐述了就绪可用软件产品安全质量各属性及其子属性的具体要求，并给出RUSP软件产品安全质量等级划分指南。

d）本部分用于指导就绪可用软件产品（RUSP）的安全质量评价。

注1：RUSP是指一种打包出售给对其特征和质量没有任何影响的需方的软件产品。典型的情况是，这种软件产品与其用户文档集一起预先包装好出售，或者从Web商店下载。用户能在任何时间通过云计算平台下载使用的软件产品都可以认为是RUSP软件产品。

注2：RUSP的例子包括但不限于：文本处理程序、电子表格、数据库管理软件、图形包以及用于技术的、科学的或实时的嵌入式功能的软件（例如实时操作系统）、人力资源管理软件、营销管理、生产管理、库存管理、智能手机应用APP、免费软件以及诸如Web网站和主页生成器之类的Web软件。

e）本部分定义了RUSP安全质量等级为CIA1-4级，其中CIA为RUSP安全质量认证的符号标识。

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。凡是注明日期的引用文件，仅注日期的版本同样适用于本文件。凡是不注日期文件的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求。

GB/T 18336.2-2015 信息技术 安全技术 信息技术安全评估准则 第2部分 安全功能要求。

GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分 安全保障要求。

GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型。

GB/T 25000.51-2016 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则。

T/SIA 008.1-2018 就绪可用软件产品（RUSP）安全质量评价标准 第1部分：软件安全质量模型。

代码安全审计规范（征求意见稿）。

3 术语和定义、缩略语

3.1 术语和定义

3.1.1

软件质量 Software Quality

在规定条件下使用时，软件产品满足明确和隐含要求的能力。

3.1.2

软件安全 Software Security

在面临蓄意威胁其可靠性的事件的情形下，软件依然能够提供所需功能的能力。

3.1.3

软件安全质量 Software Security Quality

描述了软件产品在受到它方信息安全攻击破坏的时候保护自身及所承载文件、数据的能力，即软件产品内在的本质安全特性。

3.1.4

本质安全 Intrinsic Security

指通过设计等手段使生产设备或生产系统本身具有安全性，即使在误操作或发生故障的情况下也不会造成事故的功能。具体包括失误—安全功能（误操作不会导致事故发生或自动阻止误操作），以及故障—安全功能（设备、工艺发生故障时还能暂时正常工作或自动转变为安全状态）。

3.1.5

结构安全 Secure Structures

指软件/系统的框架结构上的安全程度，包括模块组成、块间关联及交互机制的安全性。

3.1.6

安全属性 Secure Attributes

指软件产品本身固有的持久的安全特性，用于描述软件产品的安全质量。

3.1.7

就绪可用软件产品 Ready to Use Software Product(RUSP)

无论是否付费，任何用户可以不经历开发活动就能获得的软件产品。

注1：RUSP包括：产品说明（包括全部封面信息、数据表、网页信息等）；用户文档集（安装和使用软件所必需的文档），包括为运行该软件产品所要求的操作系统或目标计算机的任何配置；计算机媒体（磁盘、CD-ROM、网络可下载的媒体等）上的软件。

注2：软件主要由程序和数据组成。

注3：本定义也适用于产品说明、用户文档集，以及作为单独的制成品而被生产和支撑的软件，该软件不收取通常的商业费用和证书费用。

3.1.8

最大可容忍宕机时间 Maximum Tolerated Downtime（MTD）

指测量软件不提供预期服务的最大可容忍时间。

3.1.9

恢复时间目标 Recovery Time Object（RTO）

指当业务中断时系统或软件恢复到授权用户预期的业务状态所需要的时间。

3.1.10

静态属性初始化 Static Property Initialization

确保安全属性的默认值是恰当的，即或者是容许的，或者事实上是受限的。

3.1.11

初始化安全 Secure Initialization

为了抵御信息泄露威胁，应用程序或会话的起始和终止事件必须包含对配置信息的安全保护。应用程序配置文件必须对敏感的数据库连接设置和其它敏感的应用程序设置进行加密。为保证初始化安全，需要谨慎而明确地对初始化和全局变量的丢弃处理活动进行监控。

3.1.12

半形式化 Semi-Formal

采用具有确定语义并有严格语法的语言表达。

3.1.13

身份管理 Identity Management（IDM）

身份管理是关于数字身份信息的政策、过程、技术的结合，这些数字身份可能属于人，也可能属于非人类的系统组件（如网络、主机、应用或者服务）。

3.1.14

凭证管理 Credential Management

用户提供的用于验证的身份信息称为凭证，最常见的凭证如用户名和口令，其它形式的凭证如令牌、证书、指纹、视网膜都是凭证的具体实例。凭证管理包括凭证的产生、存储、同步、重置和撤销。

3.1.15

最小授权 Least Privilege

指系统仅授予主体完成工作所必要的访问权限。

3.1.16

职责分离 Separation of Duties（SOD）

遵循不相容职责相分离原则,没有人可以被分配两个互斥的角色,以实现组织合理分工。

3.1.17

入口点 Entrance Point

为完成预期的功能，软件需要从外界输入信息的地方，例如开放的远程过程调用（RPC）端点、开放的命名管道、Internet服务器应用程序编程接口（ISAPI）筛选器、文件和共享的弱访问控制列表（ACL）等等。

3.1.18

软件身份标签 Software Identification（SWID）Tags

指为标识软件的身份而采用的一种数字签名技术，通常由软件开发方的私钥生成。

3.1.19

多因素认证 Multi-factor Authentication

信息安全认证可以基于申请者所拥有的知识（如:口令）、物理硬件的所有权（如:智能卡）或生物特征（如:指纹）。采用上述两种或两种以上方法进行的认证被称为多因素认证。

3.1.20

使用周境 Context of Use

指用户、任务、设备（硬件、软件和原材料）以及使用某产品的物理和社会环境。

3.2 缩略语

下列缩略语适用于本文件：

RUSP：就绪可用软件产品（Ready to Use Software Product）

MTD：最大可容忍宕机时间（Maximum Tolerated Downtime）

RTO：恢复时间目标（Recovery Time Object）

SWID：软件身份标识（Software Identification）

IDM：身份管理（Identity Management）

SOD：职责分离（Separation of Duties）

4 RUSP 的安全质量要求

4.1 RUSP 的安全属性要求

根据T/SIA 008.1-2018标准的要求，对软件产品的保密性、完整性、可用性、真实性、访问授权、可记账/审计性，以及结构安全性、脆弱性、个人信息和隐私安全性等安全质量属性的要求进行阐述。

4.1.1 软件安全质量--保密性要求

用户文档集中所陈述的安全保密功能应该是可执行的。软件应符合产品说明中所阐述的安全保密功能的要求。

4.1.1.1 保密机制

指为保护数据资产不被未授权用户非法读取，所采取的加密技术或措施。保密机制如对称加密、非对称加密、信息摘要技术、数字证书技术、代码混淆技术、数字隐藏技术或掩码技术。主要包括：

a）加密算法。加密算法应该采用可验证的成熟算法，常用的加密算法包括：数据加密和解密、数字签名产生或验证、密钥校验和（用于完整性或校验和验证）产生、安全散列（哈希函数）、密钥加密和解密以及密钥协商算法等。

b）传输数据的保密性。软件应对所传输的数据/文件提供足够充分的保密性保护功能。

c）存储数据的保密性。软件应对所存储的数据/文件提供足够充分的保密性保护功能。

4.1.1.2 密钥管理

应对密钥的生成、分发、存取和销毁过程进行统一管理。具体包括：

a）密钥的生成。要求根据某个指定标准规定的算法和密钥长度来生成密钥。

注：这里“某个指定标准”是指开发方可以采用国家密码管理机构认定的商用密码算法，也可以采用行业标准建议的加密算法标准，或者企业自定义标准的成熟的加密算法。下文中出现的“某个指定标准”的含义与本条款相同。

b）密钥的分发。要求根据某个指定标准规定的分发方法来分发密钥。

c）密钥的存取。要求根据某个指定标准规定的存取方法来存取密钥。

d）密钥的销毁。要求根据某个指定标准规定的销毁方法来销毁密钥。

4.1.2 软件安全质量--完整性要求

描述软件防止未授权访问、篡改计算机程序或相关数据的能力。

4.1.2.1 软件自身的完整性

软件自身的完整性包括：

a）软件自身的完整性保护。软件应根据某个指定开发标准对软件产品进行封装，采用SWID技术对软件身份进行标识，并有对外界的修改和破坏进行感知的能力。

b）入口点安全检测。适用时，软件应该不仅能够检测应用程序入口点的安全攻击，还应该具有对物理侵害的明确检测。

c）物理组件完整性检测。适用时，软件应该能够保护组件，限制外部对软件系统中的物理设备进行未授权的物理访问，以及阻止和抵抗对该设备进行未授权的物理修改和替换。

4.1.2.2 数据/文件的完整性

数据/文件的完整性包括：

a）完整性保护算法。适用时，软件应具有对所传输、存储或处理的数据/文件进行完整性保护的能力，确保所处理的信息或数据不被未授权的人员篡改或在篡改后能够被迅速发现。可采用哈希算法或数字签名技术对数据/文件进行保护。

b）传输数据的完整性。软件应根据某个标准规定的方法对所传输的数据/文件提供必要的完整性监视功能。

c）存储数据的完整性。软件应根据某个标准规定的方法对所存储的数据/文件提供必要的完整性监视功能。为了提供数据的完整性保护，软件产品还应具有操作撤销和回退的功能。

d）撤销。当软件检测到完整性错误时，应该能够采取相应的动作对完整性进行保护，“撤销”前面的操作，“撤销”操作的参数应该是可配置的。

e）回退。当软件检测到完整性错误时，应该能够采取相应的动作对完整性进行保护，“回退”操作到前面的某一个数据是完整的步骤，“回退”操作的参数应该是可配置的。

4.1.3 软件安全质量--可用性要求

描述软件被授权实体访问并按需求使用的特性，即当需要时能存取所需的信息，而未授权的用户则无法获取信息或资源。

4.1.3.1 数据备份与复制

适用时，软件应提供对其自身以及所处理的数据具有备份和复制的能力，并在设计中对备份和复制技术给与特殊考虑，使MTD和RTO都在可接受的水平。

4.1.3.2 容错

即便发生了确定的失效，软件也能继续发挥应有的能力，维持系统正常运转。容错方式可以分为降级容错和受限容错。

注1：降级容错是指当软件发生了确定的失效时，仍然能够继续正确发挥既定能力。受限容错是指当软件发生了确定的失效时，仍然能够继续正确发挥所有能力。

注2：降级容错使软件在发生故障不能正常运行时，仍然有能力执行基本功能，以保证用户生产数据不丢失，实现基本的业务连续性保障。

4.1.3.3 故障转移

当服务或数据发生不可用的意外状态时，软件应为用户提供从一个活跃的交易软件、服务器系统、硬件或网络自动或手动转移/切换至安全的备用（冗余）系统的能力，以实现从故障中自动恢复的过程。

4.1.3.4 可扩展性

适用时，软件应该提供适当的可扩展能力，使用户在系统容量和业务能力上得到升级。这种扩展即包括垂直扩展，也包括水平扩展。

注1：垂直扩展。垂直扩展意味着将额外的资源添加到现有节点。它还升级现有的节点以处理日益增长的需求，通常涉及硬件的升级。例如为应用程序服务器增加额外的内存或存储器，或者增加连接池的设置以处理日益增长的后端数据库的连接。

注2：水平扩展。水平扩展意味着新节点被添加到现有节点。例如为软件安装新的副本，或者向已有的应用部署中添加代理缓存服务器和Web服务器。如果硬件的可扩展性受到限制，可以设计软件或系统的可扩展性来代替硬件的扩展能力。

4.1.4 软件安全质量--真实性要求

指对象或资源的身份标识能够被证实符合其声明的程度。

4.1.4.1 认证机制

软件应该能够确认或识别一个主体或资源所声称的身份，被认证的主体可以是用户、进程、系统和信息等。通过标识和鉴别确保用户与正确的安全属性（如身份、组、角色、安全性或完整性等级）相关联。主要包括：

a）身份鉴别。鉴别一个主体是他所声称的那个人，可以基于主体所拥有的知识（如口令等）、所有权（如智能卡、动态令牌卡等）和生物特征（如人脸识别、指纹识别等）。认证机制可以分为单因素认证、双因素认证以及多因素认证。

b）数据鉴别。通常指数据源发鉴别，允许实体为信息的真实性承担责任。其中包括：秘密的鉴别。

c）鉴别失败。当不成功鉴别尝试次数达到预定临界值的时候或者鉴别不成功时，软件可以自动终止会话进程;更进一步地,能够使新的尝试登陆该用户账号或登陆点(如工作站）的操作无效，直到满足管理员定义的条件才能再次激活。（“鉴别失败”也见于“4.1.7.2失效安全”）。

d）安全标记。安全标记是指对主体和客体设置的敏感标记，以区别授权用户和非授权用户访问客体对象的能力，只有授权用户可以访问客体，而非授权用户不能访问客体。应检查服务器操作系统和数据库管理系统，查看是否能对所有主体和客体设置敏感标记，这些敏感标记是否构成多级安全模型的属性库,主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理。

4.1.4.2 凭证管理

指凭证的产生、存储、同步、重置和撤销过程的安全性。为保证用户身份的唯一性，要求在执行任何动作以前,用户的身份都已被成功标识,并且用户的身份标识是与主体绑定的,且是可审计的。

4.1.4.3 抗抵赖性

抗抵赖性主要包括：

a）原发抗抵赖。软件应确保信息的发起者不能成功地否认曾经发送过信息。

b）接收抗抵赖。软件应确保信息的接收者不能成功地否认对信息的接收。

4.1.5 软件安全质量--访问授权要求

根据访问主体的身份和职能为其分配一定的权限,访问主体只能在权限范围内合法访问。

4.1.5.1 访问控制机制

指在访问主体与访问对象之间介入的一种安全机制,是对主体访问客体的权限或能力的限制。应确保软件控制范围内的任何主体和客体之间的所有操作都被一个访问控制函数覆盖。主要包括：

a）访问控制表（ACL）。软件应通过主体和客体列表，设置受控主体与受控客体之间的访问控制规则，以确定在受控主体与受控客体间的一个操作是否被允许。规则应该是基于安全属性的，明确拒绝主体访问客体的规则。

b）访问控制模型。根据安全需求说明，选择合适的访问控制模型，例如强制访问控制模型或者基于角色的访问控制模型。

c）完全中介。指每一次的访问请求都需要被仲裁，因此授权过程不能被后面的访问请求绕过。

4.1.5.2 权限管理

在身份认证后，对于谁有资格（授权或允许）执行什么操作的权限控制，包括权限授予、验证、更新和回收等权限生命周期的管理。通过访问控制表和访问能力表，决定允许授权用户（角色）的访问权限。主要包括：

a）访问权限授予。包括：

1）允许对用户组（角色组）进行管理，指定允许建立或修改安全访问权限的角色。

2）允许授权用户（角色）管理指定的安全访问权限值。

3）允许规则/策略来指定安全权限值的继承。

4）确保安全访问权限的属性值对安全状态而言是有效的。

b）权限请求超限。当用户访问请求达到或超过了设定的限值，应采取必要的动作以保证安全。

c）访问权限撤销。管理能够调用安全访问权限撤销这一功能的角色组，管理可能发生撤销的用户、主体、客体和其它资源列表，管理撤销规则。

d）访问权限到期。当系统为授权用户提供了指定的安全访问权限有效期的时候，软件应该有能力在访问权限到期时采取预先设置好的列表中的动作，如将访问权限撤销、悬挂用户账号或者删除用户访问组。

注：这里的到期时间可以依据可靠时间戳来判断。

4.1.6 软件安全质量--可记账/可审计性要求

确保一个实体的访问动作可以唯一地被区别、跟踪和记录，以用于信息系统的审计。可记账性通常是通过审计轨迹和日志来实现。对于不同的任务，软件日志记录/审计轨迹内容是不同的，附表3列出了一些审计实例。根据GB/T 25000.51-2016，可记账性一般可以分为以下几个级别进行记录：

a）最小级：对软件执行的某个操作成功；

b）基本级：对软件执行的所有操作；

c）详细级：对软件执行的某一个具体安全动作属性；

d）精细级：执行软件某一动作的主体身份。

4.1.7 软件安全质量--结构安全性要求

描述与业务流程密切相关的安全功能模块的完备性、软件架构安全性、模块之间接口安全性、以及与其他软件互联互通的安全性。

4.1.7.1 安全功能的完备性

依据软件说明书中阐述的安全目标，软件所实现的安全功能的完备程度。

4.1.7.2 失效安全

失效即保持安全状态，指软件在误操作或发生故障的情况下也不会造成事故的功能，可以通过可信恢复和自检的方式来实现。

a）可信恢复。确保软件在运行中断后能在不削弱保护能力的情况下恢复软件功能。包括：

1）手动恢复。允许软件只提供人工干预以返回安全状态的机制。

2）自动恢复。规定了对至少一种类型的服务中断，需在无人工干预的情况下自动恢复到安全状态，对其它类型的服务中断可要求手动恢复。

b）自检。适用时，软件应该能够检测多种失效和数据损坏，这些失效可能是以不可预见的方式，或由硬件、固件和软件设计上的某些疏忽造成的，也可能是由于逻辑和（/或）物理层面上的保护不当而导致软件被恶意损坏所造成的。这些检测可在软件启动时进行、或周期性地进行、或应授权用户的请求进行、或满足其他条件时进行。

4.1.7.3 资源控制

软件应保证所使用资源的安全性，包括：每一个资源应该有一个唯一的标识，重要资源在使用之前要进行正确的初始化设置，资源分配数量、使用权限和有效时间限制、资源使用过后的及时释放，以及对外部资源的完整性和真实性检查等。包括：

a）资源或变量的初始化安全。应保证RUSP软件产品的静态属性初始化安全，即应确保安全属性的默认值是恰当的，或者是容许的，或者事实上是受限的。初始化安全要求软件应采取必要的措施对初始化参数信息进行监控和保护，防止其被泄露和破坏。

注1：软件在安装部署到用户系统上时，默认状况下应进行安全的初始化，避免因为未初始化关键变量而导致系统按非预期值执行，同时避免不安全的资源或变量的初始化。例如当用户第一次登陆时应该提示用户修改密码，同时将原缺省的密码作废。

注2：结构安全性还应该说明为什么初始化过程是安全的。

b）限制资源的分配和使用。对分配的资源数量、使用权限、有限时间做限制，合理控制递归，防止消耗过多资源。

c）及时释放资源，不使用已过期或已释放的资源。及时释放系统资源，禁止再调用已释放或过期的资源，释放资源前应完全清除敏感信息。

d）残余信息保护。确保当资源从一个客体释放并重新分配给另一个客体时，其中的任何数据都不可用。本条款要求保护那些已在逻辑上删除或释放但仍可能残存在系统控制的资源中的数据，这些资源仍可能被重新分配给另一个客体。

4.1.7.4 接口安全

指用户和软件/系统或者软件的组件之间通信时，要保证接口的安全性。例如：屏幕上显示敏感信息时应该采用屏蔽技术，避免信息泄露。接口安全还包括离线存储、输入和输出安全。包括：

a）状态同步协议。对于包含分布式组件的软件，各部分组件之间存在潜在的状态差别和通信延迟，需要采用状态同步协议，保证一个组件的安全动作完成后，状态保持同步。这种状态同步协议可以通过可信回执和时间戳来实现。

b）组件之间基本安全参数值的一致性。对于包含分布式组件的软件，要求基本安全参数值（包括与数据有关的安全属性、审计信息、标识信息等）在各个组件之间复制时保持一致性。

4.1.7.5 互联互通性

描述了软件上下游之间通信的安全性。例如需要在应用程序之间共享密钥时，如果一个上游应用程序使用特定的密钥对数据进行加密，必须有一个安全的方式将密钥传送给下游的应用程序，以解密数据。包括：

a） 内部数据传送的基本保护。包括:

1） 当数据在软件内部不同部分之间传送时，软件应保护用户数据不被泄露或修改。

2）软件应该能够检测数据在不同部分之间传送时的完整性错误，包括数据的修改、数据替换、数据重排、数据删除等操作。

3）数据在检测到完整性错误之后，应该能够采取动作措施进行报警或对错误进行纠正。

b） 数据输出保护。包括：

1）输出数据的保密性。软件应防止在与另一个可信的IT产品之间转移数据时被泄露，该数据可能是一些安全关键信息，如：口令、密钥、审计数据或可执行代码。

2）输出数据的完整性。软件应防止在与另一个可信IT产品之间传送数据时被未授权修改，该数据可能是一些安全关键信息，如：口令、密钥、审计数据或可执行代码。适用时，软件应提供检测数据在与另一个可信IT产品之间传送时是否被修改的能力，假设另一个可信IT产品所使用的安全机制是已知的。软件还应具有纠正被修改数据的能力。

3）输出数据的可用性。软件应防止在与另一个可信的IT产品之间转移数据时失去其可用性，该数据可能是一些安全关键信息，如：口令、密钥、审计数据或可执行代码。

c）安全参数值的一致性。对于包含分布式组件的软件，要求基本安全参数值（包括与数据有关的安全属性、审计信息、标识信息等）在不同可信软件产品之间复制时应保持一致性，并要求对其做出一致性解释。

4.1.7.6 会话安全

适用时，软件应限制一个用户可以为某个会话选择的会话安全属性范围，保证会话的安全性。包括：

a）会话失败。对于选择会话安全属性的所有失败尝试应该记录，以备审计。

b）多重并发会话的基本限定。要求软件具有基于安全属性来限制单一用户的最大并发会话数目的能力。

c）会话锁定和终止。适用时，软件应具有对用户和软件之间交互式会话的锁定、解锁和终止的能力。

注1：会话锁定是指当用户在规定的时间内一直不活动，系统就发起一个交互式会话锁定，同时提供用户锁定和解锁其拥有的交互式会话的能力；并在会话锁定时，清除或覆写显示设备，使当前的内容不可读。除了会话解锁活动之外，终止用户数据存取/显示设备的任何活动，以保证数据安全。

注2：会话终止是指当用户在规定的时间间隔内一直不活动，系统就终止该交互式会话；或者允许用户终止自己的交互式会话。会话终止可以利用会话锁定机制，并且这种会话终止活动应该是可以审计的。

d）拒绝会话建立。适用时，软件应该能够提供拒绝用户基于属性对系统资源进行访问的要求。

4.1.7.7 可信信道

当软件需要执行关键的安全操作或者传输重要的数据时，软件应为用户和其他可信IT产品之间提供一个可信的信道，以实现数据传输的保密性。

4.1.7.8 安全的经济性

指以较低的开发成本和资源消耗获得具有较高安全质量的软件产品和系统保障。

a)从开发的角度，以风险驱动的安全开发方法降低了软件产品的安全风险，减少了软件产品安全漏洞的数量，使系统运维成本大大降低，因而降低了软件生命周期的总成本。

b)从操作的角度，指用户在使用安全的软件过程中不应该比没有安全功能之前的软件操作上更困难。

4.1.8 软件安全质量--脆弱性

指软件产品本身存在的安全漏洞或Bug，以及这些漏洞被攻击的概率和可能产生的影响。

4.1.8.1 漏洞类型

指安全漏洞分类归属的信息。根据国家标准GB/T 28458-2012《信息安全技术　安全漏洞标识与描述规范》，可以确定漏洞所属的类别。

4.1.8.2 严重度及影响分析

严重度及影响分析包括：

a）漏洞严重度。指漏洞的安全级别，可以根据国家标准GB/T 30279-2013《信息安全技术 安全漏洞等级划分指南》确定。

b）漏洞影响分析。指利用安全漏洞对目标系统造成的损害程度，可以用对基本安全属性的影响程度来描述，如对保密性、完整性、可用性的影响。

4.1.8.3 漏洞生命周期管理

针对漏洞的发现、利用、修复、公开等漏洞生命周期所进行的预防、收集、消减和发布等一系列管理活动。依据漏洞从产生到消亡的整个过程，可以将信息安全漏洞生命周期划分为以下四个阶段：

a）漏洞的发现。通过人工或者自动的方法分析、挖掘出漏洞的过程，并且该漏洞可以被验证和重现。

b）漏洞的利用。利用漏洞对计算机信息系统的保密性、完整性和可用性等安全属性造成损害的过程。

c）漏洞的修复。通过补丁、版本升级或配置策略等对漏洞进行修补的过程，使得该漏洞不能够被恶意主体所利用。

d）漏洞的公开。通过公开渠道（如网站、邮件列表等）公布漏洞信息的过程。

4.1.8.4 静态代码测试

静态代码测试是指在程序代码不运行的状态下，采用自动化代码分析工具对源程序代码的语法、结构、过程、接口等进行检查以验证程序的正确性的过程。静态代码测试的对象是

程序源代码本身，目的在于及早发现其中存在的安全Bug。源代码测试常常能够指出安全问题产生的根源，而不是简单地指出安全漏洞表现出来的外部特征。这对漏洞的修复是至关重要的。

4.1.8.5 渗透测试

渗透测试是指由安全专业人员执行的由外及内的测试，主要聚焦于最终系统配置中的漏洞。渗透测试能为发现系统管理和安全控制的漏洞提供直接的信息。对于RUSP软件产品的渗透测试可以测试软件在模拟环境下运行时所表现出来的安全漏洞问题，可以帮助软件开发人员及早识别可能在实际运行中出现的各种漏洞问题。

4.1.9 软件安全质量--隐私安全性

软件开发过程中应该保证将要处理的个人信息与隐私的安全，具体包括以下三个方面：

4.1.9.1 法律依从性

软件在处理个人信息和隐私过程中应遵从《中华人民共和国网络安全法》的与个人信息保护相关标准的内容，在个人信息的收集、使用、传输等一系列活动中实现法律遵从。

注1：下文中《中华人民共和国网络安全法》简称为“网络安全法”。

注2：“个人信息保护相关标准”是指GB/T 35273-2017《信息安全技术 个人信息安全规范》和T/SIA 001-2017 《企业个人信息安全管理规范》，下文中“个人信息保护相关标准”同此义。

4.1.9.2 透明性

软件在个人信息收集、使用、传输过程中，所实现的就是所声称的功能，并采用一定的标识实现功能的可见性。

4.1.9.3 隐私保护设计

为防止用户身份被其他用户发现并滥用，可采用匿名、假名、不可关联性、不可观察性等技术，对隐私信息进行保护。应包括：

a）匿名功能。确保用户在不暴露其身份的情况下使用资源或服务。

1）简单匿名：其他用户或主体不能确定与某一个主体或操作绑定的用户身份。

2）无索求信息的匿名：确保软件不询问用户身份来增强匿名要求。

b）假名功能。确保用户在不暴露其身份的情况下使用资源或服务，但仍能对该次使用负责。

1）可逆假名：软件提供一种可根据用户所提供的别名确定原始用户身份的能力。

2）别名假名：软件采用某种构造规则对用户身份和别名进行关联。

c）不可关联性。不可关联性要求用户和（/或）主体不能确定是否同一个用户在系统中进行了某种特定的操作。

d）不可观察性。确保一个用户在使用某个资源和服务时，其他人尤其是第三方不能观察到该资源和服务正被使用。

e）隐私保护设计的三个边界。根据网络安全法和个人信息保护相关标准，应保证软件产品的隐私设计边界，不存在欺骗性设计，避免滥用设计和危险的设计。

注1：欺骗性设计是指设计信号不真实，如虚假口头或书面陈述、误导价格要求、销售危险的、有缺陷的产品或服务而没有充分披露、未能披露有关传销的信息、使用诱饵和切换技术、未能履行承诺的服务，以及未能履行的保修义务。欺骗性设计打破信任，导致风险计算错误，使用户很难做出正确决策。

注2：滥用设计是指软件设计跨越了信息技术边界，限制了人类自主决策的能力，使他们做出将会后悔的决定。例如：利用人们的心理脆弱性和非理性，来进行产品营销或建立商业模式。

注3：危险的设计是指软件的设计使用户处于一种危险的境地，使用户容易受到他人的伤害。

4.2 产品说明要求

软件产品说明应根据T/SIA 008.1-2018包含的有关RUSP软件安全质量模型的描述，以书面形式展示可验证的安全性证据。

4.2.1 保密性

4.2.1.1 保密性说明

产品说明应根据T/SIA 008.1-2018中包含的有关保密性的陈述，对RUSP软件产品的安全保密质量属性给予文字的或半形式化的说明。

4.2.1.2 加密功能概述

产品说明应提供该产品中最终用户可调用的安全加密功能概述，包括加密机制和密钥生命周期管理。

4.2.1.3 可测试/可验证性

产品说明中包括的保密质量属性陈述应该是可测试的或可验证的。

4.2.2 完整性

4.2.2.1 完整性说明

产品说明应根据T/SIA 008.1-2018中包含的有关完整性的陈述，对RUSP软件产品的完整性质量属性给予文字的或半形式化的说明。

4.2.2.2 完整性功能概述

产品说明中应阐明软件产品的完整性机制概述，包括软件产品本身的完整性保证、所处理对象数据以及传输数据的完整性保证机制。

4.2.2.3 可测试/可验证性

产品说明中包括的完整性特征陈述应该是可测试的或可验证的。

4.2.3 可用性

4.2.3.1 可用性说明

产品说明应根据T/SIA 008.1-2018中包含的有关可用性的陈述，对RUSP软件产品的可用性质量特性给予文字的或半形式化的说明。

4.2.3.2 可用性机制概述

产品说明中应阐明软件产品的可用性机制概述,包括数据备份和复制、故障转移和可扩展性方法说明。

4.2.3.3 可测试/可验证性

产品说明中包括的可用性特征陈述应该是可测试的或可验证的。

4.2.4 真实性

4.2.4.1 真实性说明

产品说明应根据T/SIA 008.1-2018中包含的有关真实性的陈述，对RUSP软件产品的真实性质量属性给予文字的或半形式化的说明。

4.2.4.2 真实性机制概述

产品说明中应阐明软件产品的真实性机制概述,包括认证机制、凭证管理和抗抵赖性。

4.2.4.3 可测试/可验证性

产品说明中包括的真实性特征陈述应该是可测试的或可验证的。

4.2.5 访问授权

4.2.5.1 访问授权说明

产品说明应根据T/SIA 008.1-2018中包含的有关访问授权的陈述，对RUSP软件产品的访问授权质量属性给予文字的或半形式化的说明。

4.2.5.2 访问授权机制概述

产品说明中应阐明软件产品的访问授权机制概述,包括访问控制模型和权限管理。

4.2.5.3 可测试/可验证性

产品说明中包括的访问授权特征陈述应该是可测试的或可验证的。

4.2.6 可记账/审计性

4.2.6.1 可记账/审计性说明

产品说明应根据T/SIA 008.1-2018中包含的有关可记账/审计性的陈述，对RUSP软件产品的可记账/审计性质量属性给予文字的或半形式化的说明。

4.2.6.2 可记账/审计性机制概述

产品说明中应阐明软件产品的可记账/可审计性机制概述。

4.2.6.3 可测试/可验证性

产品说明中包括的可记账/审计性特征陈述应该是可测试的或可验证的。

4.2.7 结构安全性

4.2.7.1 结构安全性说明

产品说明应根据T/SIA 008.1-2018中包含的有关结构安全性的陈述，要考虑安全架构、安全功能的完备性、失效安全、接口安全、互联互通等特性，并以书面的形式展示可验证的结构安全证据。

4.2.7.2 结构安全方法概述

产品说明中应给出软件产品的结构安全性方法，以及可能影响软件结构安全的因素。

4.2.7.3 可测试/可验证性

产品说明中包括的结构安全性特征陈述应该是可测试的或可验证的。

4.2.8 脆弱性

4.2.8.1 脆弱性特征说明

产品说明中应阐明RUSP软件产品的脆弱性质量特性，并对软件的脆弱性质量特征给予文字的或半形式化的说明。

4.2.8.2 脆弱性状况概述

产品说明中应阐明RUSP软件产品的脆弱性状况概述，包括漏洞的类型、严重度及其影响、漏洞生命周期管理。

4.2.8.3 可测试/可验证性

产品说明中包括的脆弱性特征陈述应该是可测试的或可验证的。

4.2.9 隐私安全性

4.2.9.1 隐私安全性说明

产品说明应根据T/SIA 008.1-2018中包含的有关个人信息和隐私安全性方面的陈述，要考虑软件产品的个人信息和隐私安全性质量属性，从软件产品对网络安全法中个人信息和隐私保护的相关内容以及相关法律法规的依从性、透明性以及隐私保护设计三个方面来阐述RUSP的隐私安全性。

4.2.9.2 隐私保护方法概述

产品说明中应阐明软件产品的个人信息和隐私安全性状况概述，如所采用的用于保护用户个人信息的各种匿名或假名算法。

4.2.9.3 可测试/可验证性

产品说明中包括的个人信息和隐私安全性陈述应该是可测试的或可验证的。

4.3 用户文档集要求

根据ISO/IEC 9127《软件工程 用于顾客软件包的用户文档集和封面信息》，有关封面信息的段落可以用于创建用户文档集。

4.3.1 可用性

用户文档集对于该软件产品的用户应是可用的。

4.3.2 标识

4.3.2.1RUSP 软件安全质量标识

基于软件安全定义和信息安全三个基本属性，即保密性（Confidentiality）、完整性（Integrity）、可用性（Availabilty），将RUSP软件安全质量标识确定为CIA，即三个基本的软件安全属性的首写字母组合。

4.3.2.2 安全标识显示

用户文档集应显示唯一的安全质量等级标识，记为CIAi，i={1,2,3,4}。

4.3.2.3 唯一性

RUSP的安全质量应以其产品唯一安全标识指称。

4.3.2.4 可靠性

用户文档集标识的软件安全质量级别应该与软件能完成的预期安全工作任务和安全服务相符合。

4.3.3 完备性

4.3.3.1 完全安全要素

文档集应包括使用该软件必须的安全要素信息。

4.3.3.2 用户完全调用

用户文档集应说明在产品说明中陈述的所有安全功能以及最终用户能够调用的安全功能。

4.3.3.3 应急响应和恢复指南

用户文档集应给出必要的数据安全备份、应急计划方案和恢复指南。

4.3.3.4 风险管控指导

对于所有关键的软件安全功能（如出现安全故障后会对安全生产产生影响或造成重大财产损失或社会损失的高风险功能），用户文档集应提供完备的指导信息和参考信息。

4.3.3.5 安全管理说明

对用户应该执行的安全管理职能，用户文档集应给出必要的明确的说明。

4.3.3.6 文档系列说明

如果用户文档集分为若干个部分提供，在该集合中至少有一处应标识出所有的部分。

4.3.4 正确性

4.3.4.1 适当性

用户文档集中的所有信息对主要的目标用户应是适当的。

4.3.4.2 无歧义

用户文档集不应有歧义的信息。

4.3.5 一致性

用户文档集中的各个文档不应自相矛盾、互相矛盾以及与产品说明矛盾。

4.3.6 易理解性

用户文档集应采用该软件产品特定读者可理解的术语和文体，使其容易被RUSP主要针对的最终用户群理解。应通过经编排的文档清单为理解用户文档提供便利。

4.3.7 安全性

4.3.7.1 软件安全质量--保密性

用户文档集中应陈述产品说明中所列的安全加密算法和密钥管理相关内容。

4.3.7.2 软件安全质量--完整性

用户文档集中应陈述产品说明中所列的完整性相关内容，包括软件身份标签、用户数据的完整性保护机制。

4.3.7.3 软件安全质量--可用性

用户文档集中应陈述产品说明中所列的可用性相关内容，如数据备份与恢复指导。可用性也包括可用性的时间和应用条件限制，如最大可容忍宕机时间MTD和恢复时间目标RTO。

4.3.7.4 软件安全质量--真实性

用户文档集中应陈述产品说明中所列的真实性相关内容，包括身份管理、凭证管理和保留政策。

4.3.7.5 软件安全质量--访问授权

用户文档集中应陈述产品说明中所列的访问授权相关内容，包括最小授权、职责分离和权限管理。

4.3.7.6 软件安全质量---可记账/审计性

用户文档集中应陈述产品说明中所列的可记账/审计性相关内容，包括用户行为痕迹记录、日志保留策略以及审计机制。

4.3.7.7 软件安全质量--结构安全性

用户文档集中应陈述产品说明中所列的结构安全相关内容，包括安全架构类型、失效安全模式、接口安全、与其它软件互联互通的安全性，以及可信路径和安全的经济性。结构安全性还要描述这种架构为什么是安全的。

4.3.7.8 软件安全质量--脆弱性

用户文档集中应陈述产品说明中所列的软件产品相关脆弱性内容，包括关键漏洞的管理情况，可能采用的漏洞修复和升级机制。

4.3.7.9 软件安全质量--隐私安全性

用户文档集中应陈述产品说明中所列的个人信息和隐私安全相关内容，包括对《网络安全法》等相关法律法规标准的依从性、隐私数据操作的透明性，以及可能涉及的伦理问题。

5 RUSP 安全质量等级划分指南

5.1 RUSP 软件安全质量等级划分原则

通过软件安全质量模型，确定RUSP软件产品安全质量级别，可以帮助用户快速简便地判断软件的受信任程度。

a) 本标准将RUSP软件产品的安全质量划分为四个等级，记为CIA 1-4，兼顾与等级保护标准(GB/T 28448-2012)和信息产品安全性评估标准(GB/T 18336.3-2015)的兼容性。

b) 本标准与这两种标准不同之处在于，等级保护标准主要是针对系统的安全测评要求，安全组件在系统中作为独立的部分来处理，而对应用软件和软件外包的安全性没有提出明确的要求。GB/T 18336/ISO/IEC 15408主要针对软件的组件来进行安全性评价，当一个系统包含多个组件时，采用组件包（CAP）来评价组件组合的总体安全性。然而这种组合是以系统作为评价对象的，而对于RUSP软件产品来说，效果并没有那么好。这是因为一个软件中可能存在多个组件，每一种组件的安全水平可能是不一样的，根据信息安全的木桶原理，组件包的总体安全水平相当于安全水平最低的组件的安全水平值。因此根据这种方法评测出来的软件的安全性比组件的安全性要低得多，而那些安全水平值高的组件没有发挥它应有的效用，造成资源的浪费。

c) 为了给用户提供更明确的软件产品安全质量水平标识，同时减少开发方资源的浪费，减少将开发过程中引入的漏洞带入生产环节的可能性，我们提出将RUSP软件产品安全质量等级划分为CIA 1-4级，对应等级保护标准的1-4级要求，同时兼顾GB/T 18336对软件产品安全性等级（EAL 1-7级）的划分原则，给出具体的RUSP软件产品安全质量等级要求。

5.2 RUSP 软件安全质量等级说明

5.2.1 CIA 1 级（最小级）

CIA 1级适用于对RUSP产品的正确运行需要一定信心，但安全威胁又并不太被看重的场合。对于需要一种基本的安全保障级别来支持个人信息或软件完整性保护的情况，CIA 1级具有一定的价值。该RUSP安全质量级别是在利用安全功能和接口规范以及指导性文档的基础上，通过软件安全功能的开发与独立测试来获得安全支持的。CIA 1级还通过RUSP产品及相关文档中的唯一标识来提供可识别的安全质量级别。与未评估的软件产品相比，CIA 1级RUSP产品在安全保证方面有了积极的意义。

5.2.1.1 适用范围

CIA 1级适用于以下这些情况：开发者或用户在传统的商品化RUSP软件中需要一个基本的安全质量保障级别，并可以负担适当的安全工程费用。

5.2.1.2 产品说明和文档集要求

CIA 1级要求软件产品说明书中应为用户提供可理解的安全功能和安全属性规范说明。

5.2.1.3 安全属性要求

a）完整性。CIA 1级要求软件采用适当的技术手段保证软件产品自身的完整性，并对所处理的数据实现通信完整性和数据完整性保证。

b）可用性。CIA 1级要求采用适当的安全保护方法，保证软件具有一定的数据备份和容错能力。

c）结构安全性。CIA 1级要求软件产品具有结构安全性特点，可以满足软件需求说明书中的安全需求内容。CIA 1级还要求软件保证用户的会话安全，以及与外界数据交换的安全性。

d）脆弱性。在脆弱性方面，CIA 1级要求RUSP软件达到基本的静态代码漏洞测试标准要求，根据测试结果对软件漏洞进行全生命周期的管理。

e）隐私安全性。在隐私安全性方面，CIA 1级要求RUSP软件产品通过隐私声明检查，遵循国家相关法律对于个人信息与隐私保护的基本要求。

5.2.2 CIA 2级（基本级）

5.2.2.1 适用范围

CIA 2级适用于以下这些情况：开发者或用户在一个有计划的开发过程中需要一种低级到中等级别的安全性保障，在缺乏现成可用的完整的开发记录时（如在对遗留系统进行安全保护、或者不易联系到开发者的时候），仍然能够为用户提供足够的安全保障，而不需要增加过多的费用和时间投入。CIA 2级需要开发者在交付设计信息和测试结果方面提供配合。与CIA 1级相比，CIA 2级增加了保密性、真实性、访问授权、可记账性、以及隐私数据处理的透明性等内容要求，加强了RUSP软件产品的安全功能的完备性和整体结构的安全性要求，在安全保障方面提供了有意义的增强。

5.2.2.2 产品说明和文档集要求

CIA 2级要求软件产品说明书中提供可理解的安全属性说明和执行规范。

5.2.2.3 安全属性要求

a）保密性。在保密性方面，CIA 2级要求软件产品对所处理的通信数据流或数据提供保密性保证，并对密钥实行生命周期管理。

b）完整性。在完整性方面，CIA 2级要求采用安全标签（SWID）技术实现对软件产品的完整性保护，采用适当的技术手段实现通信完整性和数据完整性保证，并采用撤销和回退功能保证软件处理的数据对象的完整性。

c）可用性。在可用性方面，CIA 2级要求采用备份和复制的方法保证数据的可用性，要求软件具有容错能力以保证软件在失效状态下仍然能够安全运行，要求软件具有故障转移能力以保证业务连续性，以及要求软件具有可扩展性实现系统升级后仍可持续运行的目标。

d）真实性。在真实性方面，CIA 2级要求软件产品对访问者或数据来源进行鉴别，对认证凭证进行安全管理，并对鉴别失败的情况进行妥善的安全保护，如终止会话、限制登陆等。

e）访问授权。在访问授权方面，CIA 2级要求采用适当的访问控制模型和技术，实现对信息资产的访问控制，并且通过安全管理手段进行授权管理和审批。

f）可记账/审计性。在可记账/审计性方面，CIA 2级要求软件产品在重要的操作和过程上都需要保留操作记录，以供系统审计和法律取证所需。

g）结构安全性。在结构安全性方面，CIA 2级要求软件产品具有完备的安全结构，会话安全、互联互通的安全性，可以满足软件需求说明书中的结构安全需求内容。CIA 2级要求软件产品具有失效安全特性，即使在误操作或发生故障的情况下也不会造成事故。CIA 2级还要求软件对资源的使用进行控制，包括：资源或变量的初始化安全、限制资源的分配和使用、以及对使用后的资源及时释放，以保证系统资源的有效利用。

h）脆弱性。在脆弱性方面，CIA 2级要求RUSP软件达到静态代码漏洞测试标准要求，根据测试分析结果对不同类别漏洞进行全生命周期的管理。

i）隐私安全性。在隐私安全性方面，CIA 2级要求RUSP软件产品具有法律依从性。通过隐私声明，遵循国家相关法律对于个人信息与隐私保护的基本要求。CIA 2级要求RUSP产品满足隐私的透明性要求，即应该能够证明RUSP所执行的对于个人信息和隐私数据的处理操作就是用户隐私声明中所声称的功能。

5.2.3 CIA 3级（详细级）

5.2.3.1 适用范围

CIA 3级适用于以下情况：开发者和用户需要中等级别的安全性保障，同时要求在不进行大规模重建的情况下，可以对软件安全性进行彻底调查，并通过合理的过程风险识别和控制对开发实践进行实质性变更，从正确的安全工程中获得最大限度的保障。CIA 3级利用安全功能、结构安全性设计以及指导性文档来提供较高水平的安全保障。与CIA 2相比，CIA 3级增加了抗抵赖、残余信息保护、接口安全性、渗透测试、安全功能的经济性、以及用户隐私保护设计方面的要求，在开发过程中提供了防篡改机制，并考虑安全功能不会增加用户的总成本。

5.2.3.2 产品说明和文档集要求

CIA 3级要求软件产品说明书中提供完备的安全功能规范和安全属性说明。

5.2.3.3 安全属性要求

a）保密性。在保密性方面，CIA 3级要求软件产品对所处理的数据以及与外界环境的通信数据提供保密性保证，并对密钥实行全生命周期安全管理。

b）完整性。在完整性方面，CIA 3级要求采用安全标签技术实现对软件产品的完整性保护，并采用适当的技术手段实现通信完整性和数据完整性保证。

c）可用性。在可用性方面，CIA 3级要求采用备份和复制的方法保证数据的可用性，要求软件具有容错能力以保证软件在失效状态下仍然能够安全运行，要求软件具有故障转移能力以保证业务连续性，并要求软件具有可扩展性以实现系统升级后仍可持续运行的目标。

d）真实性。在真实性方面，CIA 3级要求软件产品对访问者或数据来源进行鉴别，对认证凭证进行安全管理，并对鉴别失败的情况进行妥善的安全保护，如终止会话、限制登陆等。CIA 3级还要求软件具有抗抵赖攻击的能力，包括原发抗抵赖和接收抗抵赖。

e）访问授权。在访问授权方面，CIA 3级要求采用适当的访问控制模型和技术，实现对数据资产的访问控制，并且通过安全管理手段进行授权管理和审批。

f）可记账/审计性。在可记账/审计性方面，CIA 3级要求软件产品在重要的操作和过程上都需要保留操作记录，以供系统审计和法律取证所需，并提供抗抵赖的能力。同时，CIA 3级标准还要求RUSP软件产品对不安全的操作和物理破坏具备审核和检查的能力。

g）结构安全性。在结构安全性方面，CIA 3级要求软件产品具有完备的安全结构，会话安全、互联互通的安全性，可以满足软件需求说明书中的结构安全性需求内容。CIA 3级要求软件具有失效安全特性，即使在误操作或发生故障的情况下也不会造成安全事故。CIA 3级还要求软件对资源的使用进行控制，包括：资源或变量的初始化安全、限制资源的分配和使用、对使用后的资源及时释放，以及对残余信息进行安全保护。CIA 3级要求软件保证其接口安全性，包括人机接口的安全、状态同步协议以及组件之间参数复制的一致性。CIA 3级还要求考虑软件安全的经济性，不会增加用户操作上的成本。

h）脆弱性。在脆弱性方面，CIA 3级要求RUSP软件达到静态代码测试和动态渗透测试标准的要求，根据测试结果对不同类别漏洞进行全生命周期的管理。

i）隐私安全性。在隐私安全性方面，CIA 3级要求RUSP软件产品具有法律依从性，通过用户隐私声明，遵循国家网络安全法对于个人信息与隐私保护的基本要求。CIA 3级要求隐私的透明性，即RUSP软件所执行的对于个人信息和隐私的处理操作就是用户隐私声明中所声称的功能。CIA 3级还要求RUSP软件产品在设计过程中考虑隐私安全，采用适当的方法对个人信息和隐私安全进行风险分析与系统设计。

5.2.4 CIA 4级（精细级）

5.2.4.1 适用范围

CIA 4级适用于安全的RUSP软件产品开发与评价，该RUSP软件将应用到高风险环境和（/或）高资产价值的情况，安全所需的额外开销与受保护资产的价值是相当的，安全属性可以通过形式化或半形式化分析方法进行验证。与CIA 3相比，CIA 4增加了软件对自身完整性风险的感知、可信信道和基于敏感性标识的数据安全保护，并且要求软件的形式化或半形式化设计开发和测试。这对于开发者或用户来说，都要在一个有计划的开发过程中需要高级别独立的安全性保障，以及较为严格的安全开发手段。

5.2.4.2 产品说明和文档集要求

CIA 4级要求软件产品说明书中提供附加错误信息的完备的形式化或半形式化安全功能规范和安全属性说明。

5.2.4.3 安全属性要求

a）保密性。在保密性方面，CIA 4级要求软件产品对所处理的数据以及与外界环境的通信数据提供保密性保证，并对密钥实行生命周期管理。

b）完整性。在完整性方面，CIA 4级要求软件产品采用安全标签技术实现对软件产品的完整性保护，并采用适当的技术手段实现通信完整性和数据完整性保证。CIA 4级还要求软件具有对入口点攻击的感知能力，限制外部对软件系统中的物理设备进行未授权的物理访问，以及阻止和抵抗对该设备进行未授权的物理修改和替换的能力。

c）可用性。在可用性方面，CIA 4级要求采用备份和复制的方法保证数据的可用性，要求软件具有容错能力以保证软件在失效状态下仍然能够安全运行，要求软件具有故障转移能力以保证业务连续性，以及要求软件具有可扩展性以实现系统升级后仍可持续运行的目标。

d）真实性。在真实性方面，CIA 4级要求软件产品对访问者或数据来源进行鉴别，对认证凭证进行安全管理，并对鉴别失败的情况进行妥善的安全保护，如终止会话、限制登陆等。CIA 4级还要求软件具有抗抵赖攻击的能力，包括原发抗抵赖和接收抗抵赖。此外，CIA 4级还要求软件提供基于安全标记的敏感数据安全保护。

e）访问授权。在访问授权方面，CIA 4级要求采用适当的访问控制模型和技术，实现对数据资产的访问控制，并且通过安全管理手段进行授权管理和审批。

f）可记账/审计性。在可记账/审计性方面，CIA 4级要求软件产品在重要的操作和过程上都需要保留操作记录，以供系统审计和法律取证所需，并提供抗抵赖能力。同时，CIA 4级标准还要求软件产品对不安全的操作和物理破坏具备审核、检查以及纠正的能力。

g）结构安全性。在结构安全性方面，CIA 4级要求软件产品具有完备的安全结构，会话安全、互联互通的安全性，可以满足软件需求说明书中的安全需求内容。CIA 4级还要求软件对资源的使用进行控制，包括：资源或变量的初始化安全、限制资源的分配和使用、对使用后的资源及时释放，以及对残余信息进行安全保护。CIA 4级要求软件保证其接口安全性，包括人机接口的安全、状态同步协议以及组件之间参数复制的一致性。CIA 4级要求软件产品为重要的信息传送提供可信信道。CIA 4级还要求软件实现安全的经济性，不会增加用户的操作成本。

h）脆弱性。在脆弱性方面，CIA 4级要求RUSP软件达到静态代码测试和动态渗透测试标准的要求，根据测试结果对不同类别漏洞进行全生命周期的管理。

i）隐私安全性。在隐私安全性方面，CIA 4级要求RUSP软件产品通过隐私声明，遵循国家相关法律对于个人信息与隐私保护的要求。CIA 4级要求软件所执行的对于个人信息和隐私的处理操作满足透明性原则，即所执行的就是隐私声明中所声称的功能。CIA 4级还要求RUSP采用适当的方法对个人信息和隐私安全进行形式化或半形式化描述、分析和设计。

6 RUSP 安全质量标准用户

本部分的用户包括：

a）软件开发方，当：

1）规定RUSP的安全需求时；

2）对照所生成的安全属性评估其软件产品时；

3）申请符合性证书或安全标识时；

b）认证/测试机构

1）希望建立某种认证模式（国际级、地区级或国家级）的认证机构；

2）遵循本标准细则提供符合性证书或安全标识而进行测试的实验室；

3）认可注册机构或认证机构以及测试实验室的认可机构；

4）可能对在安全或业务攸关的应用中使用的RUSP软件产品提出安全要求或推荐使用本部分的安全要求的监管机构；

c）潜在的需方，其可能：

1）把预期的工作任务与现有软件产品的产品说明信息进行比较；

2）需求已获认证的RUSP；

3）检验要求是否被满足；

4）可从更好的软件产品获益的最终用户。

注：在特定的使用周境中，每类用户均对使用质量和产品质量有一定的要求，表1给出了RUSP软件产品的安全质量特性清单，可供相关单位和人员使用本标准时参照。在软件开发或获取之前，宜从利益相关方的视角定义安全质量需求，并分析使用需求，由此将产生一个RUSP产品达到使用需求所需要的安全导出功能和安全质量需求。

表1　RUSP安全质量等级要求

软件安全属性	一级子属性	二级子属性	CIA 等级
4.1.1 保密性	4.1.1.1 保密机制	4.1.1.1 a）加密算法	2
		4.1.1.1 b）传输数据的保密性	2
		4.1.1.1 c）存储数据的保密性	2
	4.1.1.2 密钥管理		2
4.1.2 完整性	4.1.2.1 软件自身的完整性	4.1.2.1 a）软件自身的完整性保护	1
		4.1.2.1 b）入口点安全检测	4
		4.1.2.1 c）物理组件完整性检测	4
	4.1.2.2 数据/文件的完整性	4.1.2.2 a）完整性保护算法	1
		4.1.2.2 b）传输数据的完整性	1
		4.1.2.2 c）存储数据的完整性	1
		4.1.2.2 d）撤销	2
		4.1.2.2 e）回退	2
4.1.3 可用性	4.1.3.1 数据备份和复制		2
	4.1.3.2 容　错		2
	4.1.3.3 故障转移		2
	4.1.3.4 可扩展性		2
4.1.4 真实性	4.1.4.1 认证机制	4.1.4.1 a）身份鉴别	2
		4.1.4.1 b）数据鉴别	2
		4.1.4.1 c）鉴别失败	2
		4.1.4.1 d）安全标记	4
	4.1.4.2 凭证管理		2
	4.1.4.3 抗抵赖性	4.1.4.3 a）原发抗抵赖	3
		4.1.4.3 b）接收抗抵赖	3

表1　RUSP安全质量等级要求（续上表）

软件安全属性	一级子属性	二级子属性	CIA 等级
4.1.5 访问授权	4.1.5.1 访问控制机制	4.1.5.1 a）访问控制表	2
		4.1.5.1 b）访问控制模型	2
		4.1.5.1 c）完全中介	2
	4.1.5.2 权限管理	4.1.5.2 a）访问权限授予	2
		4.1.5.2 b）权限请求超限	2
		4.1.5.2 c）访问权限撤销	2
		4.1.5.2 d）访问权限到期	2
4.1.6 可记账/审计性			2
4.1.7 结构安全性	4.1.7.1 安全功能的完备性		1
	4.1.7.2 失效安全	4.1.7.2 a）可信恢复	2
		4.1.7.2 b）自检	2
	4.1.7.3 资源控制	4.1.7.3 a）资源或变量的初始化安全	2
		4.1.7.3 b）限制资源的分配和使用	2
		4.1.7.3 c）及时释放资源	2
		4.1.7.3 d）残余信息保护	3
	4.1.7.4 接口安全		3
	4.1.7.5 互联互通性	4.1.7.5 a）内部数据传送的基本保护	1
		4.1.7.5 b）数据输出保护	1
		4.1.7.5 c）安全参数一致性	1
	4.1.7.6 会话安全		1
	4.1.7.7 可信信道		4
	4.1.7.8 安全的经济性		3
4.1.8 脆弱性	4.1.8.1 漏洞类型		1
	4.1.8.2 严重度及影响分析		1
	4.1.8.3 漏洞生命周期管理		1
	4.1.8.4 静态代码测试		1
	4.1.8.5 渗透测试		3
4.1.9 隐私安全性	4.1.9.1 法律依从		1
	4.1.9.2 透明性		2
	4.1.9.3 隐私保护设计		3

7 附 件

附表 1 GB/T18336《信息技术 安全技术 信息技术安全评估准则》信息系统评估保障级汇总

保障类	保障族		评估保障级依据的保障组件						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
开发	ADV_ARC	安全架构		1	1	1	1	1	1
	ADV_FSP	功能规范	1	2	3	4	5	5	6
	ADV_IMP	实现表示				1	1	2	2
	ADV_INT	TSF 内部					2	3	3
	ADV_SPM	安全策略模型						1	1
	ADV_TDS	TOE 设计		1	2	3	4	5	6
指导性文档	AGD_OPE	操作用户指南	1	1	1	1	1	1	1
	AGD_PRE	准备程序	1	1	1	1	1	1	1
生命周期支持	ALC_CMC	CM 能力	1	2	3	4	4	5	5
	ALC_CMS	CM 范围	1	2	3	4	5	5	5
	ALC_DEL	交付		1	1	1	1	1	1
	ALC_DVS	开发安全			1	1	1	2	2
	ALC_FLR	缺陷纠正							
	ALC_LCD	生命周期定义			1	1	1	1	2
	ALC_TAT	工具和技术				1	2	3	3
ST评估	ASE_CCL	符合性声明	1	1	1	1	1	1	1
	ASE_ECD	扩展组件定义	1	1	1	1	1	1	1
	ASE_INT	ST 引言	1	1	1	1	1	1	1
	ASE_OBJ	安全目的	1	2	2	2	2	2	2
	ASE_REQ	安全要求	1	2	2	2	2	2	2
	ASE_SPD	安全问题定义		1	1	1	1	1	1
	ASE_TSS	TOE 概要规范	1	1	1	1	1	1	1
测试	ATE_COV	覆盖范围		1	2	2	2	3	3
	ATE_DPT	深度			1	2	3	3	4
	ATE_FUN	功能测试		1	1	1	1	2	2
	ATE_IND	独立测试	1	2	2	2	2	2	3
脆弱性评定	AVN_VAN	脆弱性分析	1	2	2	3	4	5	5

注1：GB/T 18336对安全的要求是基于组件的，每一个组件的安全等级可以分为7个EAL等级。在软件/系统安全性评价时，需要在各组件安全评估的基础之上，通过CAP即组件的组合保障包来实现系统的安全保障。该标准对组合TOE的保障定义了三个组合保障包，分别是结构组合、系统组合，测试和复查。每一个CAP由保障组件的一个适当组合组成，这三个组合保障包按级别排序。

注2：附表1中保障组件数字级别的含义：

ADV_ARC.1 安全架构描述

ADV_FSP.1 基本功能规范

ADV_FSP.2 安全执行功能规范

ADV_FSP.3 带完整摘要的功能规范

ADV_FSP.4 完备的功能规范
ADV_FSP.5 附加错误信息的完备的半形式化功能规范
ADV_FSP.6 附加形式化描述的完备的半形式化功能规范
ADV_IMP.1 TSF实现表示
ADV_IMP.2 TSF实现表示完全映射
ADV_INT.2 内部结构合理
ADV_INT.3 内部复杂度最小化
ADV_SPM.1 形式化TOE安全策略模型
ADV_TDS.1 基础设计
ADV_TDS.2 结构化设计
ADV_TDS.3 基础模块设计
ADV_TDS.4 半形式化模块设计
ADV_TDS.5 完全半形式化模块设计
ADV_TDS.6 带形式化高层设计表示的完全半形式化模块设计

附表 2 GB/T28448-2012 《信息安全技术 信息系统安全等级保护测评要求》的应用安全相关测试要求

	一级	二级	三级	四级	备注
身份鉴别	✓	✓	✓	✓	
访问控制	✓	✓	✓	✓	
授权和审批	✓	✓	✓	✓	管理要求
通信完整性	✓	✓	✓	✓	
数据完整性	✓	✓	✓	✓	
软件容错	✓	✓	✓	✓	
备份和恢复	✓	✓	✓	✓	
通信保密性		✓	✓	✓	
数据保密性		✓	✓	✓	
密码管理		✓	✓	✓	
安全审计		✓	✓	✓	
资源控制		✓	✓	✓	
变更管理		✓	✓	✓	
应急预案		✓	✓	✓	
剩余信息保护			✓	✓	
抗抵赖			✓	✓	
审核和检查			✓	✓	
安全标记				✓	
可信路径				✓	
自行软件开发					未给出
外包软件开发					安全要求

注：黄色表示一级等保开始的安全功能要求，绿色表示二级等保开始增加的安全功能要求，蓝色表示三级等保开始增加的安全功能要求，红色表示四级等保开始增加的安全功能要求。

附表 3 部分软件安全审计示例

安全属性		1 级（最小级）	2 级（基本级）	3 级（详细级）	4 级（精细级）
保密性	加密算法	密码运算的类型，加密成功和失败	所有有效的密码运算模式、主/客体属性		
	传输数据的保密性	使用数据交换机制的任何用户或主体的身份	企图使用用户数据交换机制的任何未授权用户或主体的身份	可用于识别传送或接收用户数据的名称或其它索引信息的参照表，该表可能包括与信息有关的安全属性	
完整性	存储数据的完整性	检查用户数据完整性的成功尝试，包括检查的结 果	检查用户数据完整性的所有尝试，如果成功的话，还包括检查的结果	出现的完整性错误的类型	检测到完整性错误时所采取的动作
	回退	所有成功的回退操作	执行回退操作的所有尝试	执行回退操作的所有尝试，包括回退操作类型的标识	
访问授权	访问控制	对 SFP 涵盖的客体执行某个操作的成功请求	对 SFP 涵盖的客体执行某个操作的所有请求	用于进行访问检查的特定安全属性	
	信息流控制	允许请求的信息流动的决定	请求信息流动的所有决定	用于做出信息流动执行决定的特定安全属性	根据策略目标(如降级材料的审计)而流动的信息的某些特定子集
真实性	数据鉴别	有效证据的成功生成	有效证据的未成功生成	请求证据的主体身份	产生证据的主体身份
	用户主体绑定	用户安全属性与一个主体的未成功绑定(如，创建一个主体)	用户安全属性与一个主体的成功绑定和失败绑定(如，创建一个主体的成功和失败)		
	抗抵赖	请求产生证据的用户的身份	抗抵赖服务调用	信息的标识、目的地和所提供的证据副本	请求验证证据的用户的身份

8 参考文献

[1] GB/T--- xxx，《信息安全技术 应用软件安全编程指南》（草案）.
[2] 宋明秋. 《软件安全开发-属性驱动模式》. 电子工业出版社 2016.5.
[3] HPE Security Fortify 分类法：软件安全错误.
[4] OWASP安全编码规范快速参考指南, Version 1.0，2012. 8.
[5] ISO/IEC 25010-2011. Preview Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models.
[6] ISO/IEC 25051-2014. Software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing.
[7] GB/T 22239-2008. 《信息安全技术 信息安系统安全等级保护基本要求》.
[8] GB/T 22240-2008.《信息安全技术 信息系统安全等级保护定级指南》.
[9] GB/T 30276-2013. 《信息安全技术 信息安全漏洞管理规范》.
[10] GB/T 30279-2013. 《信息安全技术 安全漏洞等级划分指南》.
[11]《中华人民共和国网络安全法》，2017.6.1实施.
[12] GB/T 35273-2017.《信息安全技术 个人信息安全规范》.
[13] T/SIA 001-2017. 《企业个人信息安全管理规范》.
[14] ISO/IEC 19770-2015. Information technology -- Software asset management -- Part 2: Software identification tag.
[15] Woodrow Hartzog. Privacy’s Blueprint. The Battle to Control the Design of New Technologies. Harvard University Press, 2018.