QJ

中华人民共和国航天行业标准

FL 1690 QJ 20103—2012

对地观测数据承载应用信息安全要求

Information safety requirements for load application of earth observation data

2013－01－04 发布 2013－05－01 实施

国家国防科技工业局 发布

前　言

本标准为对地观测数据承载应用系列标准的第一个标准，此系列标准主要由以下七个标准组成：

a)　QJ 20103-2012　对地观测数据承载应用信息安全要求；

b)　QJ 20104-2012　对地观测数据承载应用中间件要求；

c)　QJ 20105-2012　对地观测数据承载应用数据交换要求；

d)　QJ 20106-2012　对地观测数据承载应用数据分发要求；

e)　QJ 20107-2012　对地观测数据承载应用业务信息空间化处理方法；

f)　QJ 20108-2012　对地观测数据承载应用元数据要求；

g)　QJ 20109-2012　对地观测数据承载应用栅格数据处理方法。

本标准由中国航天科技集团公司提出。

本标准由中国航天标准化研究所归口。

本标准起草单位：上海九运通用软件有限公司。

本标准主要起草人：何　畏、陈根宝、陆立明、焦广武、谭　兵、王　翔。

对地观测数据承载应用信息安全要求

1 范围

本标准规定了对地观测数据承载应用信息安全的技术要求，包括数据密级、数据加解密、数据的防抵赖处理、敏感信息隐藏、访问控制、数据备份与恢复等。

本标准适用于对地观测数据承载应用系统研制和应用过程中的信息安全处理。

本标准不适用于信息安全的立法和涉密系统环境方面的信息安全处理。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包含勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GJB 2256 军用计算机安全术语

3 术语和定义

GJB 2256确立的以及下列术语和定义适用于本标准。

3.1

承载应用 load application

利用对地观测数据的空间特性创建地理空间平台，并建立平台与业务信息之间的空间关联关系，达到组织、管理、表现各类业务信息的应用模式，在该模式中不改变业务信息的任何属性，即对地观测数据承载信息应用模式。

3.2

秘密分级 security level

根据对地观测数据的时效性、分辨率、敏感程度及共享范围划分的不同保密级别。

3.3

防抵赖 non repudiation

建立有效的责任机制，防止信息的制造者和修改者在事后否认其行为。

3.4

数字签名 digital signature

以数字形式，在信息中附加签名人身份，并标明签名人认可其中内容的数据。

3.5

敏感信息隐藏 sensitive information hiding

把敏感地区数据隐藏或伪装起来，通过授权才能可见的隐藏方法，从而达到保密的一种手段。

3.6

原始数据信息隐藏 information hiding for raw data

利用图像处理工具直接对原始图像数据进行伪装或隐藏的一种信息隐藏方法。

3.7

非授权信息隐藏　conceal information for non authorization

在信息浏览时对非授权用户进行隐藏处理的一种信息隐藏方法。

4　对地观测数据的密级分级

4.1　分级原则

对地观测数据的分级应严格遵守国家保密法规，以维护国家安全，促进对地观测数据流动、促进其价值的充分发挥为原则。

4.2　分级划分

依据对地观测数据的时效性、分辨率、敏感程度等因素，将对地观测数据划分为秘密、受控和公开三个等级：

a)　秘密：不可对外公开，若泄露会使国家的安全和生产单位的利益遭受损害的数据；

b)　受控：不可向特定的群体以外人员随意公开的数据；

c)　公开：可提供公开共享的数据。

4.3　密级标识

对地观测数据的密级应作出电子标识，密级标识应包括：密级、保密期限、定级日期等。

4.4　密级标识存储

对地观测数据的密级标识应存储在每个独立的数据文件中，不应与数据文件分离存储，密级标识本身应使用加密等措施进行有效存储。

4.5　密级确认

对地观测数据的密级由数据生产单位提出建议，经生产单位主管部门审核确认。密级的变更或调整应报生产单位主管部门或上级主管部门审批，同时更改标识。

4.6　密级应用要求

密级应用应符合以下要求：

a)　不同密级的数据应执行不同的存储策略；

b)　不同密级的数据应执行不同的访问策略；

c)　不同密级的数据应接受不同程度的管理监控。

4.7　密级认证

密级认证应符合以下要求：

a)　对地观测数据在进行发布或共享时，应对密级标识进行认证；

b)　密级认证应与访问控制协同工作，通过制定相应的安全访问策略来执行数据的应用；

c)　密级认证应提供审计功能，用于记录发布对象、发布数据名、操作对象等安全相关信息。

5　对地观测数据的加密

5.1　一般要求

进行加密处理后，对地观测数据应符合以下规定：

a)　在技术设计上达到的安全等级应高于攻击者的攻击级别，使之不能破译密码；

b)　在使用管理上达到的安全保护能力应高于攻击者的攻击能力，使之难以破译密码；

c)　选择密码体制及其密码算法时，为了拥有足够的保密强度，能承受各种级别的攻击，达到实际

上不可破译，应遵循保密性强、运行效率高、方便管理和成本低等原则；

d) 建立有效的密钥管理，包括密钥的产生、存储、分配、更换、连通、分割、销毁的全过程；

e) 建立密钥的层次结构，用密钥来保护密钥，使密钥难以被盗取，即使盗取也已失去了价值。

5.2 存储数据加密

存储数据加密应符合以下规定：

a) 存储数据加密应有效地防止明文信息的泄露；

b) 存储数据加密应适应加密数据存储时间长以及不同用户访问信息时使用相同密钥的要求；

c) 应根据数据的密级、共享程度等具体情况来确定加密保护方式（局部、全局），且加密操作所占用的系统资源以及访问操作的方便性，均应在用户允许范围之内；

d) 加、解密处理应在授权用户进行读写、操作时，以透明方式进行；

e) 加、解密处理所消耗的时间应在用户应用所能承受范围之内；

f) 加、解密处理不应对非授权用户提供支持。

5.3 传输数据加密

传输数据加密应符合以下规定：

a) 对地观测数据在传输中应对数据流进行加密，以防止通信线路上的窃听、泄漏，即使传输数据被截获后也得不到数据的明文；

b) 数据传输的完整性应通过数字签名的方式来实现，即数据的发送方在发送数据的同时利用单向的不可逆加密算法 Hash 函数计算出所传输数据的消息文摘，并将该消息文摘作为数字签名随数据一同发送，接收方在收到数据的同时也收到该数据的数字签名，接收方使用相同的算法计算出接收到的数据的数字签名，并将该数字签名和接收到的数字签名进行比较，若二者相同，则说明数据在传输过程中未被修改，数据完整性得到了保证；

c) 数据在进行安全通信前，应采取身份鉴别、消息鉴别和第三方仲裁等技术手段来保证数据在传输过程的真实性和有效性；

d) 数据传输加密应支持各种传输手段和方式，且引起的数据传输延时应在用户所能承受的范围之内；

e) 加、解密处理应对用户透明或调用接口函数实现；

f) 加、解密处理不应对非授权用户提供支持。

6 对地观测数据的防抵赖处理

为了避免对地观测数据被非法复制和散发，对地观测数据应使用数字水印技术来实现防抵赖的目的，即在每个数据中嵌入数字水印，发现未经授权的拷贝，可通过这些嵌入图像内容中的信息，确认数据的创建者或购买者。

用于防抵赖的数字水印使用应满足下列要求：

a) 应有很强的鲁棒性和安全性，能抵抗恶意的擦除、伪造，除了要求在一般图象处理（如：滤波、加噪声、替换、压缩等）中生存外，还应能抵抗一些恶意攻击；

b) 应根据水印应用的具体情况确定水印的可见方式（可见、不可见），且水印添加操作所占用的系统资源以及访问操作的方便性，均应在用户允许范围之内；

c) 水印添加操作处理不应对非授权用户提供支持；

d) 进行水印检测时只能通过唯一的与数据内容相关的密钥提取出水印内容。

7 对地观测数据的信息隐藏处理

7.1 信息隐藏对象的范围

信息隐藏对象的范围包括对地观测数据中所有涉及国家安全的目标信息。

7.2 信息隐藏处理

信息隐藏处理应符合以下规定：

a) 信息隐藏处理应包括原始信息隐藏处理和非授权信息隐藏处理两种方式，处理方法的选择应根据数据的地理区域和包含涉密信息的安全等级来确定；

b) 当对地观测数据所在区域中包含的信息安全级别较高时，应使用原始信息隐藏处理，以防止信息外泄；

c) 当对地观测数据所在区域中包含涉密但授权用户可访问的重要信息时，应使用非授权信息隐藏处理，以实现数据的分权访问；

d) 原始信息隐藏处理时，应将敏感地区数据隐藏或伪装，使其不可见，且应与周围区域融合，使得处理后图像保持自然，最大程度的减少边缘效应和处理痕迹；

e) 非授权信息隐藏处理应通过信息隐藏进程来动态实现，以使请求数据中的敏感区域不可见或被伪装，且处理应与数据获取接口关联；

f) 在向外提供数据前应检测请求区域以及请求用户的浏览权限，以决定是否进行信息隐藏处理，非授权信息隐藏处理使用的算法应有较强的稳定性和较高的处理效率。

8 对地观测数据的访问控制

8.1 访问控制的策略、模型和机制

访问控制应符合以下要求：

a) 为了保护对地观测数据的可用性和完整性，防止非法用户访问、窃取与破坏数据资源，防止合法用户对数据的非法使用，以及不该拒绝合法用户访问到它有权访问的数据资源，应确立访问控制策略、模型与相应的机制；

b) 访问控制策略除识别的一次性控制外，还应包括授权的二次性控制；

c) 为了精确描述策略，应使用合适的数学模型；

d) 访问控制策略应由安全机制相应的安全功能集合来实施；

e) 要求更有效地保护两种以上的数据安全特性时（如可用性和完整性），应采用多级访问控制结构，其机制应是：

1) 安全访问规则为多种规则组成的集合，且相应地存在多个访问控制判定；

2) 对多个判定产生的结果进行处理，变成一种判定后才去执行访问控制。

8.2 身份识别与确认

身份识别与确认应符合以下要求：

a) 应对每个用户规定唯一的标识符，以识别数据访问者的身份，并通过验证手段来确认是否为合法用户，只有身份识别与确认都正确，才允许用户访问数据；

b) 要求使用口令实现确认时，正确分配给合法用户的口令应可读、难猜和安全存放，且应基于单向加密算法的密文来存储，还应采用可变口令和经常更换口令等防护措施，以防止对口令的试探性探测或在口令传送过程中被窃听后冒充合法者身份；

c) 当使用用户拥有的身份识别卡等信物实现确认时，应采用符合标准的推荐产品，其性能应能对抗冒充、猜测、伪造和穷举等攻击。对智能化、小型化的信物应优先采用。

8.3 授权控制

应划分数据密级、用户类别、数据资源类别及其访问的操作类别，并规定与数据密级、用户类别、允许访问数据资源类别及其访问的操作类型相适应的签证，以便确定相应的权限。

8.4 自主访问控制

应具有自主或强制访问控制，或者两者的结合。在自主访问控制时，用户应在被授权的情况下才能访问数据资源，且允许具有授权地位的用户根据自己的意愿将访问权授予其他用户，但应经访问控制机构的检查与认可。在实施强制访问控制时，应对用户和被访问的数据资源分配一种不能更改、唯一的安全属性，经访问控制机构进行比较、认可后，用户才能访问数据资源。

9 对地观测数据备份与故障恢复

9.1 备份分类

备份主要包括以下两类：

a) 完全备份：在正常运行时能对数据进行完全备份，应在必要时能立即投入使用；

b) 增量数据备份：在正常运行时应能定时对新增数据进行备份。

9.2 备份要求

备份应符合以下要求：

a) 对于重要数据数据备份应选择两种以上的备份介质，以增强其可靠性；

b) 对地观测数据在应用前应采用完全备份模式进行备份；

c) 对地观测数据在每次更新后应实施备份；

d) 备份文件应有备份说明，说明备份时间、该备份与其他备份的区别等信息；

e) 数据备份应授权管理员才能完成；

f) 数据备份应有备份日志，以备审计使用。

9.3 故障恢复分类

故障恢复包括以下两类：

a) 手动恢复，提供以人工干预的方法使对地观测数据承载信息应用系统数据信息恢复到安全状态的机制；

b) 自动恢复，对至少一种类型的服务中断，在无人干预的情况下能使对地观测数据承载信息应用系统数据信息恢复到安全状态。

9.4 恢复的一般程序

恢复的一般程序如下：

a) 检查数据破坏情况；

b) 选择查找恢复所需要的备份文件，选择最近时间点的数据备份文件；

c) 使用应急恢复系统对数据进行恢复；

d) 检查数据的完整性。

中华人民共和国航天行业标准

对地观测数据承载应用信息安全要求

QJ 20103—2012

*

中国航天标准化研究所出版

北京市丰台区小屯路 89 号

邮政编码：100071

中国航天标准化研究所

印务发行部印刷、发行

*

2013 年 5 月出版

定价：10 元