环境数据加密技术规定

（征求意见稿）

编制说明

《环境数据加密技术规定》编制组

二〇一〇年十月

目　　录

环境数据加密技术规定编制说明

1　项目背景

1.1．任务来源

根据《关于确定“国家环境信息与统计能力项目”技术标准规范协作单位的通知》（环信发【2009】11号），由环境保护部信息中心和四川省环境信息中心共同承担本技术规定的编制任务。

1.2．工作过程

1、　查阅资料，收集国内外相关信息安全和加密技术标准和规范；

2、　调研和收集不同安全级别的环境数据给出的数据及通讯过程的安全协议，研究国内外相关标准和规范；

3、　参加2010年1月7日在北京召开的“国家环境信息与统计能力建设项目标准规范启动暨技术交流会议”，通过会议进一步明确了项目的具体要求，并对项目有关问题进行了初步探讨。

4、　参加2010年3月3日在天津召开的“国家环境信息与统计能力建设项目标准规范启动暨技术调研会议”，对项目有关问题进行了调研讨论，明确了制定规范的原则及指导思想，细化了各规范的主要内容。

5、　参加2010年3月30、31日在北京召开的“国家环境信息与统计能力建设项目标准规范开题论证会”，在会上汇报了前期所做的工作及后期否认工作计划，听取了专家对《环境数据加密技术规定开题论证报告》及《环境数据加密技术规定大纲》（初稿）的改进意见，《环境数据加密技术规定开题论证报告》及《环境数据加密技术规定大纲》（初稿）获得了与会专家的充分肯定。

6、　2010年4月9日在成都邀请了四川省信息安全有关专家对《环境数据加密技术规定大纲》（初稿）的编制进行了指导；编制组根据专家意见对《环境数据加密技术规定大纲》（初稿）作了进一步修改、补充。

7、　参加2010年4月21日在四川召开的“国家环境信息与统计能力建设项目标准规范编制四川调研会”，会上听取了来自四川省及多个市县区环保部门代表的意见，进一步讨论了信息安全方面有关标准规范制定的原则，相关编制小组之间的协调问题，并到基层作了实地考察调研。

8、　参加2010年6月3日在内蒙呼和浩特召开的“国家环境信息与统计能力建设项目标准规范研讨会”，进一步探讨了网络和信息安全几个标准之间的协调问题并接受了标准的结构和编写有关知识的培训。

9、　在以上工作基础上，2010年6月至8月《环境数据加密技术规定》编制组编写“环境数据加密技术规定征求意见稿”及“环境数据加密技术规定征求意见稿编制说明”。

2　技术规定制定的必要性分析

2.1．国家及环保部门的相关要求

为实现“十一五”环境保护的目标，给政府决策提供全面有力的信息支持，使政府有效掌握全面信息，科学分析信息，快速做出决策，及时采取应对措施，环境保护部将实施“国家环境信息与统计能力建设”项目，提升各级环保部门环境信息与统计能力。针对目前国内还没有环境数据加密的标准，为保障“环境信息与统计能力建设项目”的建设，保护环境信息在系统中的安全，环境数据加密标准的制定是必不可少的。

2.2. 相关环保标准

HJ/T 212-2005 污染源在线自动监控（监测）系统数据传输标准

HJ/T 352-2007 环境污染源自动监控信息传输、交换技术规范（试行）

HJ/T 416-2007 环境信息术语

HJ/T 417-2007 环境信息分类与代码

HJ/T 418-2007 环境信息系统集成技术规范

HJ/T 419-2007 环境数据库设计与运行管理规范

HJ 460-2009 环境信息网络建设规范

HJ 461-2009 环境信息网络管理维护规范

HJ 511-2009 环境信息化标准指南

2.3. 标准的最新研究进展

国内目前暂时还没有针对对环境数据加密方面的标准规定。

3 国内外相关标准情况的研究

本技术规定的编写过程中参阅研究了大量国家信息安全方面相关的标准。

GB/T 18794 开放系统安全框架，第 2 部分主要是定义鉴别的基本概念、确定可能的鉴别机制类、定义用于这些鉴别机制类的服务、确定为支持这些鉴别机制类的协议的功能需求和确定鉴别的通用管理要求；第 4 部分主要是定义抗抵赖的基本概念、定义通用抗抵赖服务、确定提供抗抵赖服务的可能的机制以及确定抗抵赖服务和机制的通用管理要求；第 5 部分主要定义保密性的基本概念，确定可能的保密性机制类、定义每一类保密性机制的设施和确定为支持保密性机制类的管理要求；第 6 部分主要定义完整性的基本概念、确定可能的完整性机制类、定义每一类完整性机制的设施以及完整性机制和其支撑的服务与其它安全服务和机制的相互关系。

GB/T 15843 实体鉴别，第 1 部分规定了一个鉴别模型以及采用安全技术的实体鉴别机制的一般要求和约束；第 2 部分规定了采用对称加密算法可能的实体鉴别机制，包括单向鉴别、双向鉴别、有可信第三方和无可信第三方参加的一些机制；第 3 部分规定了采用数字签名技术单向和双向实体鉴别机制；第 4 部分规定了采用密码校验函数单向和双向实体鉴别机制；第 5 部分主要描述了三种使用零知识技术的实体鉴别机制：基于身份的机制、基于使用离散对数的基于证书的机制和基于使用非对称加密系统的基于证书的机制。

GB/T 17903 抗抵赖，提供了在证据生成、证据传输、证据存储、证据检索和证据验证阶段的抗抵赖机制，第 2 部分和第 3 部分主要描述采用对称技术和非对称技术可能的抗抵赖机制。

这些标准根据国内的实际情况而制定，对国内数据加密具有指导意义，也是国内各行业数据加密应遵循的标准。

本技术规定制定的主要依据是国家信息安全相关的标准，遵循国家有关信息安全方面的各项标准。

本技术规定的编写过程中也参考了国际标准化组织和美国国家标准 ANSI 数据加密方面的相关标准，如：

ANSI/INCITS/ISO/IEC 18033-1-2005 信息技术.安全技术.加密算法.第 1 部分:总则；

ANSI/INCITS/ISO/IEC 18033-3-2005 信息技术.安全技术.加密算法.第 3 部分:分组密码；

ANSI/INCITS/ISO/IEC 18033-4-2005 信息技术.安全技术.加密算法.第 4 部分:序列密码；

这些标准都是针对信息加密和保密传输而制定，在全世界应用广泛。

4　编制的依据与原则

4.1．编制的依据

本技术规定主要依据以下有关信息安全方面的国家标准：

GB/T 9387.2-1995 信息处理系统 开放系统互连 基本参考模型 第 2 部分：安全体系结构

GB/T 15843.1-2008 信息技术.安全技术.实体鉴别.所有部分

GB/T 15851-1995 信息技术.安全技术 带消息恢复的数字签名方案

GB/T 15852.1-2008 信息技术.安全技术.消息鉴别码.所有部分

GB/T 16264.8-1996 信息技术.开放系统互连.目录.第 8 部分:鉴别框架

GB/T 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 17902 信息技术.安全技术.带附录的数字签名.所有部分

GB/T 17903.1-2008 信息技术.安全技术.抗抵赖.所有部分

GB/T 17964-2008 信息安全技术.分组密码算法的工作模式

GB/T 18238 信息技术.安全技术.散列函数.所有部分

GB/T 18794.1-2002 信息技术.开放系统互连.开放系统安全框架.第 1 部分：概述

GB/T 18794.2-2002 信息技术.开放系统互连.开放系统安全框架.第 2 部分：鉴别框架

GB/T 18794.3-2003 信息技术.开放系统互连.开放系统安全框架 第 3 部分：访问控制框架

GB/T 18794.4-2003 信息技术.开放系统互连.开放系统安全框架.第 4 部分：抗抵赖框架

GB/T 18794.5-2003 信息技术.开放系统互连.开放系统安全框架.第 5 部分：机密性框架

GB/T 18794.6-2003 信息技术.开放系统互连.开放系统安全框架.第 6 部分：完整性框架

GB/T 20271-2006 信息安全技术.信息系统通用安全技术要求

GB/T 20273-2006 信息安全技术.数据库管理系统安全技术要求

GB/T 22239-2008 信息安全技术.信息系统安全等级保护基本要求

GB/T 22240-2008 信息安全技术.信息系统安全等级保护定级指南

4.2．编制的原则

本技术规定的制定以等级保护为核心，根据 GB/T 17859-1999 、GB/T 22239-2008 和 GB/T 22240-2008 国家标准，国家环境信息与统计能力建设项目中信息系统应达到其规定的第三级要求，信息系统中非涉密敏感数据应达到第三级所要求的安全标准。

制定的标准能适用于国家环境信息与统计能力建设项目中信息系统中的各种数据加密过程，既能保证数据信息的安全又同时容易使用。

5　技术路线

《环境数据加密技术规定》从机密性、完整性、抗抵赖性和认证四个方面规定了国家环境信息与统计能力建设项目下所属信息系统中非涉密数据可使用的机制。

5.1．数据机密性

按照 GB/T 17859-1999 第三级安全标准对数据机密性的要求，应采用加密或其它有效措施实现系统管理数据、鉴别信息和重要业务数据传输和存储保密性并通信过程中的整个报文或会话过程进行加密。

数据的机密性可以通过访问控制使只有授权实体才能访问数据，通过加密或编码保护数据的语义。数据加密的主要体系有：

1）　对称加密体系

其主要特点是：加解密双方在加解密过程中要使用完全相同的一个密钥，该密钥也称保

密密钥，需要双方共同保密。对称算法的效率比较高，适合大批量的数据加密。常用的这类算法有 AES、DES、IDEA 和 RC2 及 RC4 等

2） 非对称加密体系（公钥加密体系）

公钥加密体系的特点：第一就是用户可以把用于加密的钥匙公开地分发给任何人；其次它允许用户事先把公开钥匙发表或刊登出来；第三它不仅改进了传统加密方法，还提供了传统加密方法不具备的应用，就是数字签名的公开鉴定系统。常用的算法有 RSA、DSA 等算法。

5.2. 数据完整性

按照 GB/T 17859-1999 第三级安全标准对数据机密性的要求，应能够检测到系统管理数据、鉴别信息和重要业务数据在传输和存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

数据完整性主要是防止或检测未授权的数据修改，包括未授权的数据创建和删除等，保护数据及其相关属性的完整性。可以通过对称、非对称密码技术或差错检测等技术实现完整性目的。

5.3. 数据抗抵赖性

按照 GB/T 17859-1999 第三级安全标准对数据机密性的要求，应具有在请求的情况下为数据原发者或接收者提供数据原发证据及数据接收证据的功能。

抗抵赖性是要生成、收集、维护已声明的事件或动作的证据,并使该证据可得并且确认该证据,以此来解决关于某事件或动作发生或未发生而引起的争议。抗抵赖性可以通过数字签名等技术实现。

5.4. 认证性

按照 GB/T 17859-1999 第三级安全标准对数据机密性的要求，在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证，本规定中还要求在通信过程中应保证数据来源的可靠性。

认证性是证实某事是否真实或是否有效的一个过程，用来确保数据发送者和接收者的真实性以及数据的完整性，阻止对数据的主动攻击。

6 主要技术内容

6.1. 适用范围

本技术规定确定了国家环境信息与统计能力建设项目中信息系统中非涉密数据的机密性、完整性、抗抵赖性和认证的要求；本技术规定适用于国家环境信息与统计能力建设项目中信息系统中非涉密数据关于机密性、完整性、抗抵赖性和认证的实现过程。

6.2. 术语和定义

本技术规定中所使用的术语和定义均采用国家相关标准中所使用的术语和定义。

6.3. 标准结构框架

本技术规定由 4 章组成，主要内容如下：

第一章为适用范围：描述了本技术规定的技术规定和适用范围；

第二章为术语和定义：列出了在本技术规定中出现的相关术语和定义出自哪些国家标准；

第三章为技术内容：描述了对数据机密性、完整性、抗抵赖性和认证的要求，各自的应用范围、实现方法、机制分类和实现的机制，本技术标准中的技术内容均基于国家相关的标准确定。

第四章为参考文献：列出了在制定本技术规定过程中所参考过的国家标准。

7　对实施本技术规定的建议

（1）数据的保密除了选用恰当的技术体制，还应该有配套的规章制度来保障，本技术规定的实施也需要建立和完善相应的信息安全方面的管理措施，从制度和技术两方面来保证系统中数据的安全。

（2）不同安全级别的环境数据，对数据保密性、数据完整性、数据不可抵赖性和认证的要求可能不同，在实施本技术规定时，应综合考虑环境数据的安全级别、环境数据的安全威胁、安全需求、网络环境等因素，从实际出发，使用本技术规定所描述的机制或它们的组合，兼顾安全与效率，使得系统所采用的安全措施既能够有效保证数据保密性、数据完整性、数据不可抵赖性和认证方面的要求，又能够容易使用，尽可能在数据机密性与易用性之间取得较好的平衡。

（3）实现过程中应使用国家安全保密部门批准使用的有关算法。