环境身份认证技术规定

（征求意见稿）

编制说明

《环境身份认证技术规定》编制组

二〇一〇年十月

目　　录

《环境身份认证技术规定》编制说明

1 项目背景

随着信息技术的发展与应用，信息系统安全的内涵在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，信息安全访问控制显得愈来愈重要。为了实现环境信息化过程中信息资源的安全共享、信息整合、互联互通的统一身份认证技术，需建立环境身份认证技术规定。

1.1 任务来源

《环境身份认证技术规定》编制项目来源于环境保护部国家环境信息与统计能力建设项目（环信发[2009]11 号）文件下达的标准规范制定计划。

《环境身份认证技术规定》编制单位是环境保护信息中心、青岛市环境信息中心、青岛通软网络科技有限公司。

1.2 工作过程

在环境保护部下达《环境身份认证技术规定》编制任务后，成立了编制组，编制小组围绕环境身份认证技术规定展开了初步的文献调研工作，了解了国际、国内相关方面的最新研究成果，并积累了一定的相关资料。在文献调研取得一定成果的基础上，编制小组开展了内部交流与讨论，总结材料、分享认识，编制小组内部形成了对本规定的范围、目的、建设原则共同的认识，并形成了本规定编制的任务书。

在形成任务书的基础上，编制小组积极寻求外部力量的支持，多次组织环境领域、信息化领域的专家对编制任务书进行评审，并提出补充与优化建议，进一步明确和完善了《环境身份认证技术规定》编制任务。

编制组从资料收集整理、技术路线的制定到编制开题报告、本规定初稿、本规定征求意见稿等，有效地开展一系列的工作。

编写《环境身份认证技术规定》开题报告，论述本规定制定的研究内容、相关标准的国内外研究现状，工作进展，确定工作内容安排及时间进度。

编写《环境身份认证技术规定》初稿，对环境身份认证的内容、形式及相关的管理办法等方面制定规范。

2010 年 3 月 30 日国家环境信息与统计能力建设项目办公室标准组在环保部 209 会议室进行了开题报告论证会，对下一步工作的开展提出了具体要求。

2010 年 4 月为展开一步的工作，与编制《环境信息安全技术规范》、《环境数据加密技术规定》和《环境数据访问技术规定》的小组成员在四川环境保护厅进行了交流与讨论，对相互间关联的内容进行了确定。

2010 年 8 月参加了环保部信息中心组织的调研活动，根据环保部指导思想按照建设 RA 的标准重新对初稿进行调整，通过总集建设方案展开对标准规范包含内容、应用范围、技术要求、证书格式、接口应用等方面进行详细论证，最后根据国家电子政务外网 CA 建设各位专家的建议以及同环保部信息中心各位领导的沟通最终确定标准规范主要从两个方面进行编写：1、RA 设备机房建设以及管理流程以及相应管理办法;2、同应用系统接口和实施方面，不在对证书格式以及实际接口方法和应用范围进行详细描述，全部引用或者参照现有 CA 建设以及国家目前现有的相关标准。

2010 年 9 月 23 日形成了《环境身份技术规定》初稿。

2010 年 10 月 22 日形成了《环境身份技术规定》征求意见稿。

2 制订的必要性分析

2.1 国内外信息安全标准的需要

国际上信息安全标准化工作兴起于 20 世纪 70 年代中期，80 年代有了较快的发展，90 年代引起了世界各国的普遍关注。目前世界上有近 300 个国际和区域性组织制定标准或技术规则，与信息安全标准化有关的组织主要有以下：

ISO(国际标准化组织) 负责制定的标准主要是开放系统互连、密钥管理、数字签名、安全评估等方面的内容；

ITU(国际电信联盟)负责研究网络安全标准，包括通信安全项目、安全架构和框架、计算安全、安全管理、用于安全的生物测定、安全通信服务等。

国内 CITS（信息技术科学学院）组织成立于 1984 年主要负责信息安全的通用框架、方法、技术和机制的标准化及归口国内外对应的标准化工作，其中技术安全包括开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口等。2004 年我国《电子签名法》出台，该法案将“电子签名”的有效性以法律形式确定下来，为信息身份认证技术的实现提供了法律的依据。

上述国内外相关标准或法律的出台，为环境信息身份认证技术标准的制定做好了铺垫。

环境保护部全力推进“环境信息与统计能力建设项目”过程中，提出了 27 项环境信息化建设的标准制定工作，“环境身份认证技术规定”是重要的基础性规范，其目的是保障环境信息资源的安全共享、信息整合和互联互通提供保障，这一标准编制工作是环境信息化建设的基础保障，组织并完善制定此标准，具有十分重要的现实意义。

2.2 环境信息互联互通的需要

随着信息化建设的快速发展，互联网的应用已经深入到社会经济生活的各个领域。以网络化、数字化环境为依托的电子商务、电子政务作为信息经济和知识经济的产物，有力地推动了世界经济的发展与繁荣，已成为全球最具活力的新的经济增长点。但是由于电子商务、电子政务是在互联网络这种开放的网络环境中生存的，如何保证互联网应用的规范、有序和安全已成为阻碍电子商务、电子政务发展的最大瓶颈。

在环保行业相关的环境信息应用系统、环境信息政务系统也面临着同样的问题。为此建立环境身份认证标准实现信息资源的安全共享、信息整合和互联互通是迫在眉睫的。

2.3 深化环保信息化建设的需要

目前国家-省-市-县各级环境保护部门的环境相关业务系统及数据量已经具有相当的规模，但是这些数据在不同部门及不同区域之间共享水平还有待提高，而环境管理形势的变化要求能够利用全国性的或多区域的数据进行数据共享、数据交换及数据决策，这要求我们必须有统一环境身份认证体系实现统一身份认证确保数据共享、交换的安全性和合法性。建立环境身份认证技术标准，这是环保信息化过程中迫切需要解决的问题。

3 国内外相关标准情况的研究

3.1 主要国家、地区及国际组织相关标准情况的研究

1、PKI 的标准

PKI(Pubic Key Infrastructure)是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。用户可利用 PKI 平台提供的服务进行安全通信。

使用基于公钥技术系统的用户建立安全通信信任机制的基础是：网上进行的任何需要安全服务的通信都是建立在公钥的基础之上的，而与公钥成对的私钥只掌握在他们与之通信的

另一方。这个信任的基础是通过公钥证书的使用来实现的。公钥证书就是一个用户的身份与他所持有的公钥的结合，在结合之前由一个可信任的权威机构 CA 来证实用户的身份， 然后由其对该用户身份及对应公钥相结合的证书进行数字签名，以证明其证书的有效性。

PKI 必须具有权威认证机构 CA 在公钥加密技术基础上对证书的产生、管理、存档、发 放以及作废进行管理的功能，包括实现这些功能的全部硬件、软件、人力资源、相关政策和操作程序，以及为 PKI 体系中的各成员提供全部的安全服务。如：实现通信中各实体的身份认证、保证数据的完整、抗否认性和信息保密等。

PKI 的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。

2、X.509 标准

X.509 是国际电信联盟-电信（ITU-T）部分标准和国际标准化组织（ISO）的证书格式标准。作为 ITU-ISO 目录服务系列标准的一部分，X.509 是定义了公钥证书结构的基本标准。1988 年首次发布，1993 年和 1996 年两次修订。当前使用的版本是 X.509 V3，它加入了扩展字段支持，这极大地增进了证书的灵活性。X.509 V3 证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段，即使在强制字段中，X.509 证书也允许很大的灵活性，因为它为大多数字段提供了多种编码方案。X.509 V4 版已经推出。

X.509 标准在 PKI 中起到了举足轻重的作用，PKI 由小变大，由原来网络封闭环境到分布式开放环境，X.509 起了很大作用，可以说 X.509 标准是 PKI 的雏形。

3、PKCS 系列标准

PKCS 是由美国 RSA 数据安全公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书作废表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。到 1999 年底，PKCS 已经公布了以下标准：

PKCS#1：定义 RSA 公开密钥算法加密和签名机制，主要用于组织 PKCS#7 中所描述的数字签名和数字信封[22]。

PKCS#3：定义 Diffie-Hellman 密钥交换协议[23]。

PKCS#5：描述一种利用从口令派生出来的安全密钥加密字符串的方法。使用 MD2 或 MD5 从口令中派生密钥，并采用 DES-CBC 模式加密。主要用于加密从一个计算机传送到另一个计算机的私人密钥，不能用于加密消息[24]。

PKCS#6：描述了公钥证书的标准语法，主要描述 X.509 证书的扩展格式[25]。

PKCS#7：定义一种通用的消息语法，包括数字签名和加密等用于增强的加密机制，PKCS#7 与 PEM 兼容，所以不需其他密码操作，就可以将加密的消息转换成 PEM 消息[26]。

PKCS#8：描述私有密钥信息格式，该信息包括公开密钥算法的私有密钥以及可选的属性集等[27]。

PKCS#9：定义一些用于 PKCS#6 证书扩展、PKCS#7 数字签名和 PKCS#8 私钥加密信息的属性类型[28]。

PKCS#10：描述证书请求语法[29]。

PKCS#11：称为 Cyptoki，定义了一套独立于技术的程序设计接口，用于智能卡和 PCMCIA 卡之类的加密设备[30]。

PKCS#12：描述个人信息交换语法标准。描述了将用户公钥、私钥、证书和其他相关信息打包的语法[31]。

PKCS#13：椭圆曲线密码体制标准[32]。

PKCS#14：伪随机数生成标准。

PKCS#15：密码令牌信息格式标准[33]。

4、WindowsCardSpace

Windows CardSpace”——原名为“InfoCard”，微软取代用户 ID 和密码成为验证网络使用者身份的新方法。说白了这就是一项以用户为中心的身份识别技术。用户可以通过它控制登

录网站时提交的信息，这将会使管理个人信息更加简便安全。同时这项技术也将包含在 Windows Vista 之中。微软推广它的目的就是取代传统的用户名和密码，因为它可以提供更好的反钓鱼功能，并且预防其他类型的网络诈骗。

3.2 国内标准情况的研究

身份认证技术已经在国内的各个行业中得到广泛应用。目前国内已存在一系列的身份认相关的法律和标准。

1、相关法律和法规

《中华人民共和国电子签名法》

中华人民共和国信息产业部令第 35 号 《电子认证服务管理办法》

2、行业应用标准

DB 42/T 362－2006 电子政务术语

GB/T 2260 中华人民共和国行政区划代码

GB/T 20518-2006《信息安全技术 公钥基础设施数字证书格式》

HJ/T 416 环境信息术语

YD/T 1322.3-2004 电子商务技术要求 第三部分：证书及认证系统

《国家政务外网注册服务点（RA）建设指南 v8.1》

《国家政务外网证书认证机构（CA）命名空间规范 v7.0》

《国家政务外网证书认证机构（CA）系统接口规范 v7.0》

中华人民共和国信息产业部颁布的《电子认证业务规则规范（试行）完全版》

3.3 制订的基本原则

《环境身份认证技术规定》的制定需要遵循以下原则：

本规定的编制与管理遵循国家环境保护部于 2006 年 8 月 31 日公布的《国家环境保护标准制修订工作管理办法》。

按照规范的标准编制过程开展标准研制工作，包括项目开题及总体方案编制、资料调研、征求意见稿编制、送审稿编制、报批稿编制和质保期阶段。

本规定的编写严格按照 GB/T 1.1-2009《标准化工作导则 第 1 部分：标准的结构和编写》的要求。

本规定的编写符合《中华人民共和国电子签名法》中设计的条款。

本规定的编写符合中华人民共和国信息产业部令第 35 号 电子认证服务管理办法中的规定。

本规定的编写要与 DB 42/T 362－2006 电子政务术语一致。

本规定的研究要参考国际先进经验保证科学性，要充分掌握内涵保证准确性，要深入了解工作流程保证系统性，要多方求证和修订保证其普遍适用性。

4 制订的技术内容

4.1 适用范围

本技术规定规定了环境身份认证数字证书格式和业务管理流程及管理办法。

适用于电子认证服务机构、数字证书认证系统及相关产品的供应商、应用开发商的设计和开发。

适用于全国各环境保护部门的身份认证。

本规定的环境身份认证数字证书格式适用于认证机构证书、环境个人证书、环境机构证书、环境设备证书、环境服务器证书、环境应用系统证书。

本规定不涉及任何具体的密码运算，所有密码运算均在符合国家有关法律法规的密码设备中进行。

本规定凡涉及密码相关内容，按国家有关法律法规实施。

4.2 结构框架

《环境身份认证技术规定》共有 10 章和 4 个附录组成，主要内容如下：

第一章为适用范围：概述了本规定的编制目的和适用范围。

第二章为术语和定义：列出了在本标准中出现的相关术语及其定义。

第三章规定了身份认证证书的格式。

第四章为认证机构（CA）命名空间的规范。

第五章为证书认证机构（CA）系统接口的规范。

第六章为证书注册机构（RA）建设规范。

第七章为证书注册机构（RA）业务流程及管理办法。

第八章为证书注册机构（RA）管理与操作安全控制。

第九章为证书受理点（LRA）建设规范。

第十章为证书受理点（LRA）管理。

规范性附录 A 为证书存储介质技术要求。

资料性附录 B 为软硬件设备参数要求。

资料性附录 C 为安全认证网关的要求。

资料性附录 D 数字证书注册机构和受理点建设样例

4.3 术语和定义

4.3.1 证书认证机构（CA）

负责创建和分配证书，受用户信任的权威机构。用户可以选择该机构为其创建密钥。

4.3.2 公钥基础设施（PKI）

支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。

4.3.3 证书注册机构（RA）

RA 是 CA 的组成部分，对证书申请的业务受理审核子系统概称为 RA，RA 按照 CA 制定的政策和管理规范对用户的资信进行审查，以决定是否为该用户发放证书。

4.3.4 证书受理点（LRA）

证书受理点 LRA 是 RA 系统的延伸，分布在环保部各下属省厅，有效地分担部机关 RA 系统的业务操作，具有录入、审核、管理及制证等功能。通过在各下属省厅布署受理点，实现为相应的下属省厅的人员就近提供便捷、迅速的证书申请、审核和发放等服务。

4.3.5 密钥管理中心（KMC）

密钥管理中心。主要负责数字证书用户密钥的生成和管理，解决系统密钥和数字证书用户密钥自产生到最终销毁的整个生命周期中的相关问题。

4.3.6 在线证书状态协议（OCSP）

在线证书状态协议，是 IETF 颁布的用于检查数字证书在某一时间是否有效的标准。

4.3.7 依赖方

即指依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。

4.3.8 公钥证书

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

4.3.9 证书吊销列表(CRL)

一种由证书签发者所认定的无效证书的清单。

4.3.10 终端实体

不以签署证书为目的而使用其私钥的证书主体或者证书使用者。

4.3.11 环境数字证书

用来标识环境信息参与方真实身份的数字证书，根据参与方的不同类别分为认证机构证书、个人证书、机构证书、设备证书、服务器证书、应用系统证书。

4.3.12 个人证书

颁发给参与环境信息的个人实体，用来唯一标识个人实体真实身份的数字证书。

4.3.13 机构证书

颁发给参与环境信息的机构实体，用来唯一标识机构实体真实身份的数字证书。

4.3.14 设备证书

颁发给参与环境信息的设备实体，用来唯一标识设备实体真实身份的数字证书。

4.3.15 服务器证书

颁发给参与环境信息的服务器实体，用来唯一标识服务器实体真实身份的数字证书。

4.3.16 应用系统证书

颁发给参与环境信息的应用系统实体，用来唯一标识应用系统实体真实身份的数字证书。

4.4 认证证书的格式及命名规范

认证证书格式规范包括数字证书基本格式、个人证书格式、机构证书格式、设备证书格式。详见《国家政务外网数字证书格式规范 v7.2》。

认证机构（CA）命名空间规范包括了个人数字证书主体信息、机构数字证书主体信息、设备数字证书主体信息、代码签名数字证书主体信息。详见《国家政务外网证书认证机构（CA）命名空间规范 v7.0》。

环境身份认证技术规定系统接口包括数字证书应用接口体系结构、数字证书应用接口组成和功能说明和数字证书应用接口函数定义。详见《国家政务外网证书认证机构（CA）系统接口规范 v7.0》。

4.5 认证注册机构的建设规范

按照国家政务外网注册服务点（RA）建设要求下发的文件为依据，对机构名称、办公场地、机房、人员配置、人员培训、节点（RA）的系统功能和机构等进行了规范。

4.6 认证注册机构（RA）业务流程及管理办法

规定了数字证书的签发、数字证书的使用、数字证书的维护、数字证书的载体、数字证书实体的查询、数字证书更新请求的确认、数字证书废止请求的确认、数字证书恢复请求的确认等

4.7 证书注册机构（RA）管理与操作安全控制

包括物理安全控制、流程安全控制、日志审计、归档策略、密钥转换等内容的规定和规范。

4.8 证书受理点（LRA）建设规范和管理办法

包括身份认证网关、目录服务器系统、加密机、USB KEY 及证书受理点人员配置和管理。

5 拟开展的主要工作

5.1 主要工作内容

1、制定总体工作计划

在本规定编制开始之前需要制定切实可行的总体工作计划，内容主要有调研计划、本规定编制工作计划，确定项目期间的工作成果及里程碑，同时确定项目参与人员及其分工。

2、本规定调研工作

本规定调研工作分为两个步骤的工作，分别是制定调研计划和确定调研方式。

制定调研计划，包括调研对象、调研内容、调研时间安排等。调查问卷中应包括本规定应用现状、需求及意见建议等内容。

确定调研方式，重点部门以现场调研/访谈为主，其他部门以问卷发放、回收为主，辅之以电话沟通。可进行专家访谈，必要时召开专家座谈会。查阅和收集互联网和图书馆文献，进行本规定资料收集整理和分析。

3、本规定编制工作

根据调研结果，进行整理汇总。明确本规定的适用范围、本规定内容，形成本规定的编制思路，然后参照规范编制方法和编制规则编制标准规范初稿。经汇报交流讨论，提交征求意见稿及编制说明。

4、征求意见稿、送审稿、报批稿完善

将规范征求意见稿发送给相关部门和人员，征求对编制的规范的意见和建议。根据征求的意见和建议，对规范进行修改并进一步完善规范内容。整理提交规范送审稿及编制说明，组织召开专家审议会，对规范的编制情况进行评审。

5.2 工作计划及时间进度安排

完成时间	工作内容
2010 年 3 月	完成规范前期研究，细化规范内容，完成开题汇报
2010 年 5 月	完成标范大纲及初稿编制
2010 年 8 月	初稿评审，修改完善形成征求意见稿及编制说明
2010 年 10 月	根据征求意见修改完善规范，整理提交规范送审稿及编制说明，组织专家评议
2010 年 11 月	根据专家评审意见整理提交规范报批稿及编制说明
2010 年 12 月	报批并发布

6 拟提交的工作成果

《环境身份认证技术规定》征求意见稿及编制说明

《环境身份认证技术规定》送审稿及编制说明

《环境身份认证技术规定》报批稿及编制说明

《环境身份认证技术规定》应用指南