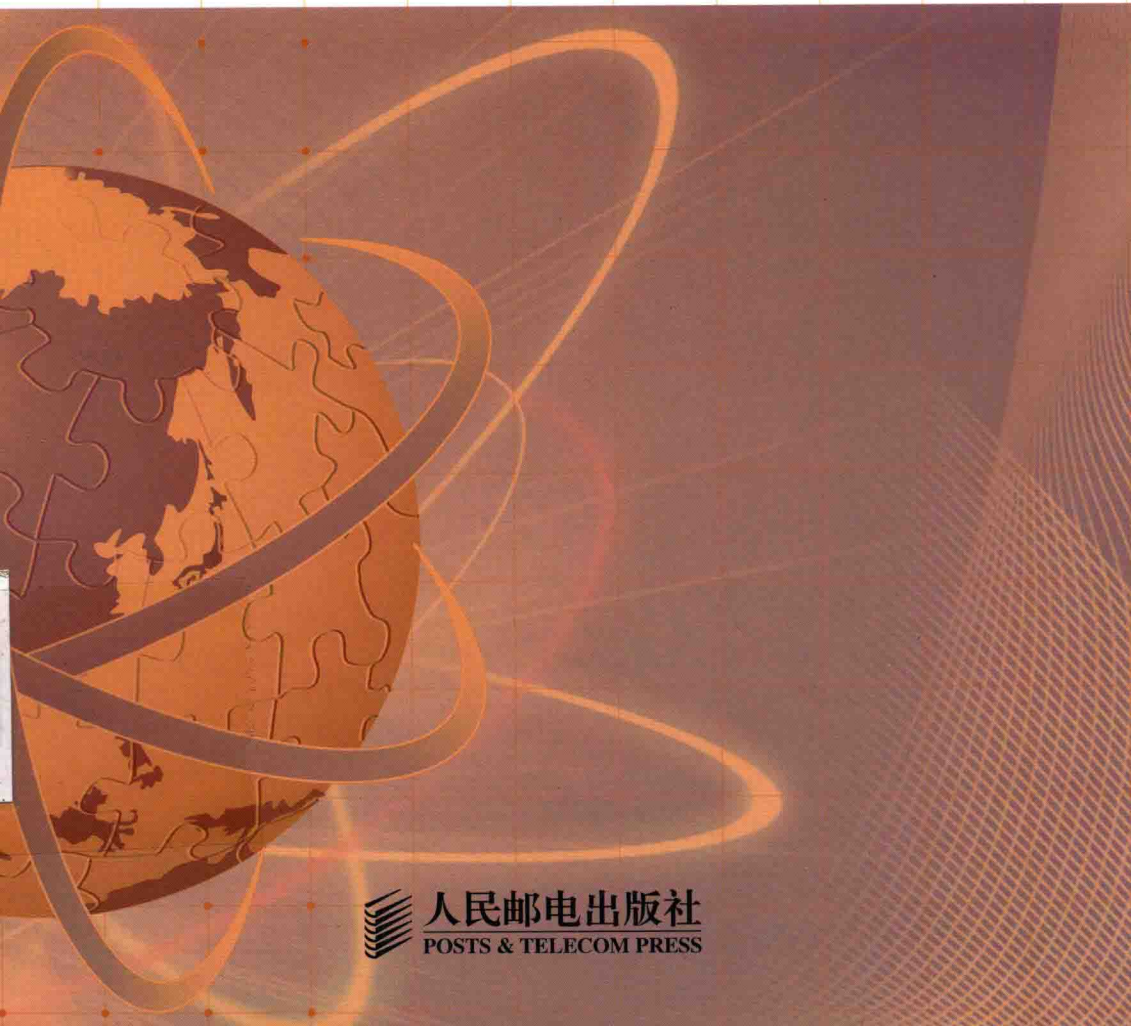
Global Network Identity Management: Current Status and Development

全球网络身份管理的现状与发展

胡传平　邹翔　杨明慧　严则明　等◎编著



人民邮电出版社
POSTS & TELECOM PRESS

Global Network Identity Management:
Current Status and Development

全球网络身份管理的现状与发展

胡传平　邹翔　杨明慧　严则明　等◎编著

人民邮电出版社
北京

图书在版编目（CIP）数据

全球网络身份管理的现状与发展 / 胡传平等编著
. -- 北京 : 人民邮电出版社, 2014.1(2014.1 重印)
ISBN 978-7-115-33491-6

Ⅰ. ①全… Ⅱ. ①胡… Ⅲ. ①计算机网络管理－研究
Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2013)第251321号

内 容 提 要

本书从网络身份管理的基本概念入手，对世界各国网络身份管理现状、国际标准化组织及机构研究现状进行了全面介绍，重点分析了网络身份管理的技术体系、网络电子身份标识及相关实例，并对网络身份管理的技术发展趋势进行了展望。

本书是根据作者近年来在网络身份管理方面的研究成果和实践经验而写成的，对网络身份管理相关研究与开发工作具有指导意义，对信息安全工程师和相关安全工作者有很好的参考价值。

◆ 编　　著　胡传平 邹　翔 杨明慧 严则明　等
责任编辑　邢建春
责任印制　杨林杰
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷
◆ 开本：700×1000　1/16
印张：14.5　　2014 年 1 月第 1 版
字数：282 千字　　2014 年 1 月河北第 2 次印刷

定价：59.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第 0021 号

序

随着互联网应用在世界各国的迅猛发展，网络空间已经成为一种新的社会形态，而网络身份虚拟性的深层次社会影响已成为各国政府关注的焦点，美国、欧盟及其成员国、俄罗斯等都已从战略计划、技术研发、标准制定、法律法规等方面大力推进网络身份管理工作。

提及网络身份管理，我们很容易将之等效于“网络实名制”。实际上，网络实名制是一种政策，是政府部门对网络管理所采取的一种模式，是将网络虚拟身份与社会物理身份相对应的一种要求；网络身份管理则是对网络身份唯一性判定、真实性鉴别的一种能力要求。网络身份管理在对网络用户管理时，可以采用基于公民网络电子身份标识（eID）的管理模式来支持网络实名制的管理要求。同时，网络身份管理所面对的还可以是网络设备、企事业法人、官方代表等具有特定网络身份的角色。因此，网络身份管理与网络实名制之间虽有些相通之处，但更多的是区别。

本书明确给出了网络身份管理的基本概念，并介绍了欧盟、亚洲、北美洲及大洋洲的各国在网络身份管理方面的法律法规、管理机制、关键技术与实施情况，以及国内外网络身份管理标准化研究现状，网络身份管理技术的模型、体系架构和关键技术，同时介绍了基于eID的网络身份管理模式。由此，从网络身份管理的各个侧面向读者展示了其历史渊源，相关国家的法律法规、国家战略规划、技术标准以及具体实施情况，介绍了世界各国网络身份管理发展现状和趋势，向读者深入浅出地揭开网络身份管理的本质。尤其是书中以比利时和德国发行基于eID的个人身份卡为实例进行了详细介绍和分析，以便让读者更深入地了解国际社会对网络身份管理的重视，以及所采取的管理模式及相应的技术手段。

当前，我国已经普遍实施网络实名制管理政策，但尚缺少强有力的技术支持。国家高技术研究发展计划（“863”计划）在“十二五”期间设立了公民网络电子身份标识方面的重大项目，作者所带领的团队是该重大项目的课题承担单位，是我国试行基于eID的网络身份管理模式的重要技术支撑力量。作者在网络身份管理

领域进行了长期的研究，并具有大范围应用试点的实践积累，在网络身份管理方面形成了深厚的积淀。本书总结了世界各国网络身份管理推进路线的共性趋势和一般规律，就我国网络身份管理的推进路线提出了科学、合理的建议，展现了作者对网络身份管理中前沿动态和相关科学问题的深入思考。相信本书有助于加深读者对网络身份管理概念和本质的认识，并引发关于我国网络身份管理推进路线的一些思考和共鸣。

中国工程院院士 方滨兴

2013 年 9 月 10 日于北京

Preface 前言

网络空间中用户身份的确认已成为大多数互联网业务的前提，然而，网络身份也面临着被盗用、滥用、泄漏等安全问题，由此造成了日益严重的安全和隐私威胁。2011 年底，发生了国内最大的开发者技术在线社区 CSDN 用户数据库泄露事件，黑客在互联网上公布了 600 万 CSDN 用户的注册邮箱账号和对应的明文密码数据。自此，中国互联网有史以来波及面最广、规模最大、危害最深的泄密事件全面爆发。随后，天涯、网易、人人、猫扑、多玩等多家大型网站的用户数据陆续被公布，规模达到千万量级。该事件的愈演愈烈，为我们揭示出围绕网络身份的一条巨大的黑色产业链的冰山一角。无独有偶，2011 年 7 月，韩国门户网站 Nate 和社交网站 Cyworld 遭到黑客攻击，导致 3 500 万用户信息外泄，包括用户姓名、ID、手机号码、E-mail 地址、加密后的居民登录证号和密码等数据，而韩国人口不到 5 000 万，意味着全国超过 70%的公民身份信息遭到了外泄。

随着互联网与现实生活联系越来越紧密，网络身份的重要地位将日益突显，所面临的安全威胁也将不断增大，不仅关系到我们个人的隐私、财产安全等方面，大规模的网络身份数据也影响到国家和社会安全，因此如何安全应用、保护和管理我们的网络身份已变得越来越重要。

在近年的工作实践中，我们深感在互联网时代保护个人网络身份安全的重要性，这不仅需要全社会的共同参与，全体网民增强自我身份保护意识，而且需要构建全方位的网络身份管理体系。笔者在近年来网络身份管理方面的研究成果和实践经验基础上，整理总结编写了本书。全书共分 10 章，简单介绍如下。

第 1 章就网络身份管理的基本概念以及现实需求进行综述。

第 2 章～第 4 章分别介绍欧洲、亚洲、北美洲及大洋洲的各国在网络身份管理方面的法律法规、管理机制、关键技术，以及各国政府网络电子身份标识计划的推行与实施情况。

第 5 章主要介绍国内外网络身份管理标准化研究现状及国际标准化组织的相关研究成果。

第 6 章详细阐述网络身份管理技术的模型、体系架构和关键技术，并进行了实例说明。

第 7 章介绍基于网络电子身份标识的网络身份管理，包括网络电子身份标识的概念、承载与发行形式、应用模式、试点项目等。

第 8 章和第 9 章分别以比利时和德国发行结合网络电子身份标识的个人身份卡为实例进行详细介绍和分析。

第 10 章就我国网络身份管理的推进路线进行了分析，并对网络身份管理的技术发展趋势进行展望。

本书由胡传平、邹翔、杨明慧、严则明等负责策划、编写和通稿。

本书的编写得到公安部第三研究室网络电子身份技术研究团队全体成员的大力支持，参加研究和写作的成员还有：汪志鹏、胥怡心、姚静晶、倪力舜、胡永涛、金波、黄道丽、丁建华、陈兵、王福、陈慧，在此表示衷心感谢。感谢直接参与本书文字编辑、校对等工作的同济大学硕士生饶洁、刘孟占、黄苏扬、李铭洋。

本书凝聚了作者长期的网络身份管理工作的实践经验以及研究思考的成果。作者广泛收集了国内外相关材料，参考了大量最新论著，在本书编写过程中也引用了部分材料，在此表示感谢。

作者

2013 年 9 月于上海

目录 Contents

第1章 Chapter 1

网络身份管理综述

以互联网为代表的众多网络环境已日渐成为日常生活的基本元素。中国互联网信息中心（CNNIC）《第32次中国互联网络发展状况统计报告》显示，截至2013年6月底，我国网络用户总数达到了5.91亿，网站达294万个，互联网普及率为44.1%[1]，信息获取、商务交易、交流沟通、网络娱乐等应用，满足了我们在互联网时代的各种需求。在现实生活中我们使用身份证、护照、企业组织机构代码等证明自己或者代表企业的身份，而在接入和使用各类互联网业务时，如发送电子邮件、使用网上银行、网上购物、在线游戏、网上聊天等，也都需要使用各种网络身份的完成注册、登录、认证和传输等操作，网络身份已日渐成为我们获取各类个性化互联网服务的必备元素。

1.1 什么是网络身份管理

1.1.1 网络身份管理的基本概念

身份的本身意义指是谁，是什么样的人。人类社会最初身份只是个体成员交往中识别个体差异的标志和象征。在现实社会，普遍使用身份证、户口簿、护照等作为对个人进行身份标识的方式。而在互联网上，我们在访问各种互联网应用中所使用的网络身份标识（如用户ID、网络ID、电子邮件地址、网游账号等）为安全验证提交给互联网应用服务提供方的身份信息（姓名、身份证号等）以及我们所声称的社会身份等，形成了“网络身份”，也称为“数字身份”。

根据维基百科中的定义，身份管理（IdM，identity management）即管理各类个人识别码，包括身份认证、授权和权限管理等过程，可以是在系统内部，也可以跨系统或跨企业边界使用，其目的是在提高安全性和生产效率的同时，降低成本、缩短停机时间和减少重复的任务[2]。网络身份管理是在网络空间中实施身份管理，用以实现网络空间的各类主体（个人用户、企业用户、互联网服务提供方等）的相互识别，如同在现实空间中使用居民身份证来证明自己的身份或鉴别对方一样。

全球许多国家都将在网络空间中实施身份管理作为关系其未来发展的重要工作任务。各国政府推行网络身份管理的驱动因素很多，主要包括构建电子政府、维护社会安全、改善社会福利、保护电子商务安全以及网络交易安全等。

网络身份管理所涵盖的范围包括如下几方面。

1）网络身份的产生，即用户如何获取自己的网络身份，例如用户自行指定、互联网服务提供方生成、第三方身份服务提供方生成等，身份可以采用标识符、数字证书等形式。

2）网络身份的保护，即如何防止网络身份被盗用或冒用，例如以密码口令形式保护银行账号或电子邮箱、以生物识别技术验证网络身份、以数字证书形式签发网络身份，以及在网络身份使用过程中使用安全的网络协议。

3）网络身份的使用，即在进行网络操作时需要出示何种形式或安全级别的网络身份，如何进行网络身份验证。

4）网络身份的维护，包括网络身份的修改、更换、挂失、恢复、注销等，即网络身份生命周期的管理。

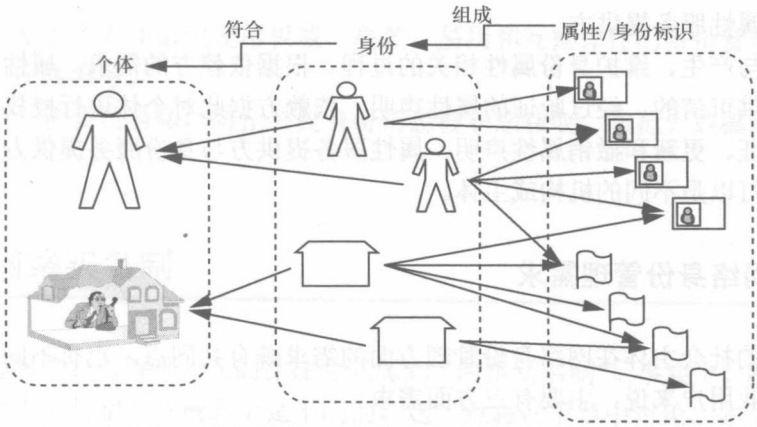
1.1.2 网络身份管理的参与方

网络身份管理的参与方主要包括内容如下。

（1）个体

个体指使用网络在线业务的个人用户。广义上，个体可以扩展到同样需要使用网络在线业务和身份鉴别的非个人实体，可以是一个机构、硬件、软件或服务。个体具有的网络身份（也称数字身份）是指在线业务中标识特定主体的一系列属性。属性是描述个体内在所具有的或者被归属的某种特征或特性（例如，个体的年龄至少是 18 岁）。个体、身份和属性间关系如图 1-1 所示。

如图 1-1 所示，个体或者其代表的企业可以拥有一个或者多个身份，由个体选择使用何种身份，而这些身份由不同的属性和身份标识组成，不同的身份包含的属性集通常会有交集。当个体代表企业的时候，他可以拥有企业的部分属性，而此时企业的属性集也可以包含其法人代表。



（来源：http://en.wikipedia.org/wiki/Identity_management）

图 1-1　个体、身份和属性间关系

（2）身份服务提供方

负责产生、维护、保护与个体相关的数字身份，也称为身份提供商。身份提供商发放在线业务中用于证明主体身份的身份标识，其中验证和登记个体真实身份的过程一般由具有权威性和公信力的登记机构来开展；并且，身份服务商需要在必要时能够对数字身份进行修改、更换、挂失、恢复、注销等。

（3）身份标识及载体

身份标识用于在网络在线业务中证明个体身份，一般被存储在物理或者虚拟形态的设备或者对象中，此设备或对象也称为身份载体。身份载体可能有多种形式，例如智能卡、智能密码钥匙、集成在 PC 中的安全芯片、移动电话 SIM 卡等形式的硬件载体，也可以以软件数字证书、软件令牌等形式存在。身份载体可被用于存储一个或多个身份标识、声明或者与对应个体相关的属性。身份载体及身份标识的选择和使用，依赖于不同的应用，也依赖于参与方对风险的分析与评估。同个体真实身份的验证和登记过程一样，与个体真实身份绑定的身份载体的发放，应由具有权威性和公信力的机构来开展。此外，身份标识在使用时也可以以链接形式提供，链接到该个体的权限、角色、特权以及其他属性。

（4）依赖方

一般指各类网络应用服务提供方，依赖方根据其对个体身份标识和属性的接收与验证，做出与业务相关的判断。依赖方根据实际业务需要确定身份服务提供方和属性服务提供方。面向不同业务，依赖方可以选择不同身份服务提供方提供的、不同安全强度的主体身份标识。此外，依赖方通常还需要向在线业务主体标识和鉴别自己的身份，以实现业务双方的相互鉴别。

（5）属性服务提供方

负责与产生、维护身份属性相关的过程。根据依赖方的需求，属性提供商向依赖方提供可信的、经过验证的属性声明，依赖方据此对个体进行授权。属性维护包括验证、更新和撤销属性声明。属性服务提供方与身份服务提供方可以是同一个，也可以是不同的机构或主体。

1.1.3 网络身份管理需求

不同的社会主体在网络身份管理方面的需求既有共同点，也有不同点。对于个人或企业用户来说，主要有三方面需求。

一是便利。个人可以方便地完成网络身份验证过程以获得网络服务，需要用户记忆、输入以及操作的过程尽量简化，获得良好的用户体验。在当前的网络环境中，个人需要自行维护大量的用户名和密码信息。优化网络身份验证用户体验的一个很好的例子就是“单点登录”，用户只需要登录一次就可以访问所有相互信任的应用系统。这种情况虽然在一定程度上减轻了用户的负担，但是往往会导致密码的重复使用行为，从而使在线欺诈和身份盗用更容易发生。

二是安全。保护个人网上活动的安全，降低个人网络身份被盗用或冒用的风险，使个人能够安心地进行网络在线工作、消费和娱乐，从而既能保证个人网上活动的保密性、完整性和可用性，又能保障关键业务的不可抵赖性，避免由于身份被窃取而造成个人财产损失或其他安全威胁。

三是隐私。在网络空间保持个人身份的私密性及匿名性，对于增强个人隐私保护和维护公民自由是至关重要的。要确保各类互联网服务提供方在一定范围内收集个人信息，仅仅使用和分发业务必需的信息，对收集、存储的个人信息实施具有足够安全强度的保护，防止个人信用、财产的损失或个人隐私信息的泄露。

对于互联网服务提供方来说，主要有两方面需求。

一是确认用户身份的真实性和有效性。确认用户确实拥有其所声称的身份或具有其所宣称的身份属性（例如年龄大于 18 岁），从而提供相应的业务，杜绝虚假身份和身份欺诈以及由此造成的交易纠纷等。

二是身份管理方案的经济性。身份管理方案应具有高性价比，能够有效降低互联网服务提供方的身份管理成本和用户身份隐私信息泄露的风险。当前大多数互联网服务提供方使用的都是相对脆弱的用户名和密码，即使如此，所需要的身份管理和保护成本也是日渐增加的，已成为一种沉重的负担。

对于政府来说，主要有三方面需求。

一是维护国家安全和社会安全，有效遏制网络欺诈、身份盗窃和在线信息滥用的增长，防止由此造成的个人或组织的财产、名誉等各类损失。