金融标准化系列丛书-4

《网上银行系统信息安全通用规范》解读

◎ 主编　李东荣

INTERPRETATION OF THE GENERAL SPECIFICATION OF INFORMATION SECURITY FOR INTERNET BANKING SYSTEM

中国金融出版社

金融标准化系列丛书-4

《网上银行系统信息安全通用规范》解读

◎ 主编　李东荣

INTERPRETATION OF THE GENERAL SPECIFICATION OF INFORMATION SECURITY FOR INTERNET BANKING SYSTEM

中国金融出版社

责任编辑：吕　楠
责任校对：刘　明
责任印制：程　颖

图书在版编目（CIP）数据

《网上银行系统信息安全通用规范》解读（《Wangshang Yinhang Xitong Xinxi Anquan Tongyong Guifan》Jiedu）/李东荣主编．—北京：中国金融出版社，2013.2
ISBN 978-7-5049-6681-0

Ⅰ.①网…　Ⅱ.①李…　Ⅲ.①电子银行—信息系统—信息安全—规范—中国　Ⅳ.①F832.2-39

中国版本图书馆 CIP 数据核字（2012）第 278330 号

出版发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　（010）63266347，63805472，63439533（传真）
网上书店　http://www.chinafph.com
（010）63286832，63365686（传真）
读者服务部　（010）66070833，62568380
邮编　100071
经销　新华书店
印刷　保利达印务有限公司
尺寸　169 毫米×239 毫米
印张　13.5
字数　248 千
版次　2013 年 2 月第 1 版
印次　2013 年 2 月第 1 次印刷
定价　49.00 元
ISBN 978-7-5049-6681-0/F.6241
如出现印装错误本社负责调换　联系电话（010）63263947

一、主编

李东荣

二、编委（按姓氏笔画排序）

于　玫　王永红　李　丹　李文辉　李晓枫　张永福

杨　竑　陆书春　罗　凯　罗　锐　贺　林　徐光贤

谢翀达

三、统稿

姜云兵　王小青

四、编写人员（按姓氏笔画排序）

王小青　王　钊　王晓燕　王海涛　仇宁宁　孙茂增

李明浩　李海滨　杜　磊　陈广辉　赵方萌　董贞良

序　言

标准化是为在一定范围内获得最佳秩序，对现实问题或潜在问题制定共同使用和重复使用的条款的活动。在现代经济发展过程中，标准化成为一国提升企业核心竞争力、争取发展话语权的重要途径。世界主要发达国家已逐渐将标准化提高到了国家发展战略的高度，成立专门从事标准化工作的组织，开展标准化工作，将发展中的成功经验，通过标准化的形式固化下来。

党中央、国务院历来高度重视标准化工作，并将标准化提高到了国家发展战略的高度，多次就标准化工作作出重要指示。金融作为现代服务业的重要组成部分、现代经济的“血液”，已成为衡量某个国家或地区综合竞争力和现代化标准的重要标志，对于标准化的要求显得更为迫切、更为重要。改革开放以来，我国金融标准化经过近二十年的发展，已逐步成为保证金融业规范化经营、提高整体核心竞争力的重要基础性条件。作为国家的中央银行，中国人民银行承担着制定和执行货币政策、维护金融稳定、提供金融服务的重要职责。随着金融改革的逐步深入，经济市场化程度的不断加深，金融标准化的地位和作用日益提高。在各相关单位的大力支持、积极参与下，中国人民银行和全国金融标准化技术委员会以立足现状、适度前瞻、突出重点、务实可行为原则，在金融领域内稳步推进标准化工作，陆续制定和发布了多项涉及银行、保险、证券、银行卡、征信业务等内容的国家标准和行业标准。同时，根据信息系统建设标准先行的指导原则，推出了一系列标准规范。

为使广大业内工作者和社会各界多渠道、多层次地了解中国金融标准化成果、标准化相关政策法规、国际标准化发展趋势等方面的内容，中国人民银行决定出版《金融标准化系列丛书》。经过精心的准备和各方面的共同努力，这套

丛书现在可以陆续和大家见面，该丛书的出版必将有力地推动我国金融标准化的发展，为大家提供有益的参考。希望可以借此推动社会各界更好地了解金融标准化，并希望金融标准化在全社会的关心支持下，在全行业人员的共同努力下，得以更好、更快的发展，为金融业持续、健康、创新发展奠定基础。

中国人民银行副行长

全国金融标准化技术委员会主任委员

二〇一二年九月

前　言

随着网上银行等电子银行业务的不断拓展，网上银行的安全性成为各方关注的焦点，为切实提升网上银行系统信息安全水平，引导网上银行业务健康发展，保护金融消费者权益，中国人民银行发布了《网上银行系统信息安全通用规范》（JR/T 0068—2012）。

《网上银行系统信息安全通用规范》是网上银行系统建设和改造升级的安全依据，也是各单位开展安全检查和内部审计的依据。为提高网上银行系统建设、改造、测评、检查和审计人员对《网上银行系统信息安全通用规范》的理解，以及增强网上银行系统信息安全技术和管理能力，能更好地开展网上银行系统信息安全建设、整改和测评工作，中国人民银行撰写了《〈网上银行系统信息安全通用规范〉解读》。

本书中第1章至第4章从网上银行系统适用的范围、参考和引用的规范、使用的术语、涉及的符号和缩略语等方面进行解读；第5章对网上银行系统的各个组成部分应实现的功能和应达到的安全目标进行要求，并从系统结构方面进行详细解读；第6章从安全技术、安全管理、业务运作三个方面对网上银行系统从管理到建设到运维提出的详细要求进行解读。

希望本书能方便大家理解网上银行系统信息安全通用规范，并对网上银行系统的建设、改造、测评、检查、审计工作有所帮助，也希望为社会大众普及网上银行系统安全知识等方面起到积极作用。同时，本书也存在诸多不足，希望在今后的使用过程中不断改进和完善，我们将会及时对其进行修订。我们恳切希望参阅本书的广大读者能够提出宝贵的意见。

编写组

二〇一二年八月

目　录

引　言

【原文】本标准是在收集、分析评估检查发现的网上银行系统信息安全问题和已发生过的网上银行案件的基础上，有针对性提出的安全要求，内容涉及网上银行系统的技术、管理和业务运作三个方面。

本标准分为基本要求和增强要求两个层次，基本要求为最低安全要求，增强要求为本标准下发之日起的三年内应达到的安全要求。各单位应在遵照执行基本要求的同时，按照增强要求，积极采取改进措施，在规定期限内达标。

本标准旨在有效增强现有网上银行系统安全防范能力，促进网上银行规范、健康发展。本标准既可作为网上银行系统建设和改造升级的安全性依据以及各单位开展安全检查和内部审计的依据，也可作为行业主管部门、专业检测机构进行检查、检测及认证的依据。

［解读］《网上银行系统信息安全通用规范》（以下简称《规范》）的引言部分对标准的编制依据、主要内容、主要功能以及执行时间要求进行说明。

《规范》编制依据：一是依据中国人民银行对网上银行信息安全管理工作实践与经验的总结和提升；二是依据近三年网银安全案件形成的调研报告；三是依据中国人民银行对国内商业银行网上银行系统安全检查评估中发现的问题，从正面提出的规范性要求。

《规范》执行要求：考虑到国内金融机构的网上银行水平不一、实现方式各异和改造周期长等特点，《规范》把内容分为基本要求和增强要求两个层次。基本要求为最低安全要求，增强要求为规范下发之日起三年内应达到的安全要求。金融机构应遵照基本要求，同时积极采取改进措施，在规定的三年期限内达到增强要求，推动网上银行安全稳定的发展。

《规范》的功能：一是建设及改造依据，网上银行系统所有者和建设方开展系统建设及改造升级的依据；二是安全测评依据，测评机构开展网上银行系统安全测评的依据；三是安全检查及内部审计依据，主管部门以及机构内部相关部门开展制度性安全检查及内部审计的依据。

1 范围

本章节主要对《规范》所包含的内容和适用的范围进行明确说明，便于读者了解《规范》的使用范围。

【原文】本标准包含了网上银行系统的描述、安全技术规范、安全管理规范、业务运作安全规范。本标准适用于网上银行系统建设、运营及测评。

［解读］本条是对《规范》中包含的内容进行概括说明。

《规范》主要从安全技术、安全管理、业务运作三个方面，对网上银行系统从管理到建设再到运维提出详细要求，这些要求是网上银行系统应达到的目标。《规范》不仅适用于网上银行系统信息安全建设，也适用于网上银行系统的架构设计、运营维护、安全测评等方面。

2 规范性引用文件

本章节对《规范》中所引用的文件进行描述，并明确第 3 章部分术语的出处。

【原文】下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术术语

［解读］本条对《规范》中引用的参考文件及其版本进行说明。

为保证《规范》中使用的名词术语、符号统一且具有规范性，在此参考国家标准 GB/T 25069 信息安全技术中术语部分的内容。

3 术语和定义

为避免和其他文档中的术语和定义混淆，本章节主要针对《规范》中关于网上银行系统和信息安全的部分术语和定义进行解释。

【原文】GB/T 25069 确立的以及下列术语和定义适用于本文件。

［解读］本条对《规范》中使用的术语范围进行说明。

GB/T 25069 是国家质量监督检验检疫总局和国家标准化管理委员会于 2010 年 9 月 2 日发布，2011 年 2 月 1 日开始实施的国家推荐标准。该标准界定了信息安全技术领域相关的概念术语和定义，并明确这些条目之间的关系。该标准适用于信息安全技术概念的理解，以及其他信息安全技术标准的制定和信息安全技术的国内外交流。

《规范》在引用 GB/T 25069 中术语的同时，也对与网上银行系统相关的常用术语进行解释，这些术语有：

3.1 网上银行（Internet Banking）

【原文】商业银行等金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供网上金融业务的服务。

［解读］本条对《规范》内提到的“网上银行”从其提供服务的主体、服务依赖环境及方式等方面进行定义。

网上银行有两层含义：一是通过信息网络开办业务的银行，这类银行没有营业厅、柜台等银行机构实体，所有业务均通过互联网或其他公共信息网络处理，是一种新兴银行体制；二是传统银行通过信息网络提供的金融服务，包括传统银行业务和信息技术应用带来的新兴业务。

《规范》中的网上银行均为第二层含义。银行通过互联网、移动通信网络等通讯环境除为客户提供余额查询、对账、转账等传统业务外，还能提供支票、信用卡、个人理财等新兴业务。网上银行具备服务方便、快捷、高效、经营成本低、使用方便等特点。

3.2 互联网（Internet）

【原文】因特网或其他类似形式的通用性公共计算机通信网络。

［解读］本条对互联网从形式上进行定义。

本条需要明确的是，互联网包含因特网。凡是具有通用性且能彼此通信的设备组成的网络即可称做互联网。《规范》中提到的互联网多指因特网。银行在互联网上开展网上银行业务，可以更方便、更快捷地为客户提供金融服务，并有利于吸引和保留优质客户、扩大客户群、开辟新的利润来源。

3.3 敏感信息（Sensitive Information）

【原文】主要指影响网上银行安全的密码、密钥以及交易敏感数据等信息，密码包括但不限于转账密码、查询密码、登录密码、证书的 PIN 等，密钥包括但不限于用于确保通讯安全、报文完整性等的密钥，交易敏感数据包括但不局限于完整磁道信息、有效期、CVN、CVN2、证件号码等。

［解读］本条对网上银行系统中敏感信息的范围进行定义。

敏感信息是一个较为宽泛的概念，一切由权威机构确定的、必须受保护的且其泄露、修改、破坏或丢失会对人或事产生可预知损害的信息都可被称做敏感信息。《规范》中将网上银行系统中涉及的敏感信息归纳为密码、密钥和交易敏感数据三大类，但并非仅有这些信息是敏感信息。在网上银行系统实际建设中，系统架构、业务需求的不同使网上银行系统中涉及的敏感信息也不同，需要系统设计者和建设者根据具体情况进行具体分析。银行应采取有效措施，保证敏感信息的机密性、完整性和可用性。

3.4 客户端程序（Client Program）

【原文】为网上银行客户提供人机交互功能的程序，以及提供必须功能的组件，包括但不限于：可执行文件、控件、静态链接库、动态链接库等，不包括 IE 等通用浏览器。

［解读］本条对网上银行系统客户端程序进行定义。

客户端程序需要由客户下载并在操作终端中安装使用，其提供的主要功能是：

（1）为客户提供操作界面；

（2）预处理/缓存部分运算请求，减少服务器资源使用；

（3）通过实施安全机制，保护敏感信息、交易数据和客户信息的安全性。

采用 IE 或其他浏览器软件作为客户端操作界面的网上银行系统多为浏览器/服务器（B/S）架构，其附加的敏感信息保护、身份认证、客户端进程保护等用来提高客户端安全性的组件均属于客户端程序的范畴。

3.5 USB Key

【原文】一种 USB 接口的硬件设备。它内置单片机或智能卡芯片，有一定

的存储空间，可以存储用户的私钥以及数字证书。

［解读］本条对 USB Key 的存在形式进行定义。

USB Key 是一种遵循即插即用接口规范的硬件设备，在网上银行系统中又被称做移动数字证书、U 盾等，是存储客户身份鉴别信息的载体。USB Key 本身具有用于运算的芯片，当客户进行资金类交易时，USB Key 通过其内置运算芯片，使用证书对交易数据进行签名后发送给网上银行服务器端，从而保证数据传输过程中的真实性和完整性，防止客户敏感信息被篡改。

3.6 USB Key 固件（USB Key Firmware）

【原文】影响 USB Key 安全的内置在 USB Key 内的程序代码。

［解读］本条对 USB Key 固件的范围进行定义。

USB Key 本身具备交易数据签名、多种算法的加解密运算、个人私钥更新等客户操作的功能，在 USB Key 内部，负责驱动内部硬件设备、密钥管理、加解密运算等可能会影响到 USB Key 自身安全性的代码均属于固件。

3.7 移动终端（Mobile Terminal）

【原文】本标准中特指区别于传统 PC 机方式，以手机、平板电脑等通过通信网络访问网上银行的移动设备。

［解读］本条对移动终端的范围进行定义。

移动终端也可称做移动通信终端。从广义范围上讲，手机、笔记本、平板电脑、POS 机甚至包括车载电脑等都可以划入移动终端的范围。《规范》中的移动终端主要是指具有多种应用功能的智能手机、平板电脑等可以访问网上银行系统的移动设备，但不排除其他新兴移动设备。

3.8 强效加密（Strong Encryption）

【原文】一个通用术语，表示极难被破译的加密算法。加密的强壮性取决于所使用的加密密钥。密钥的有效长度应不低于可比较的强度建议所要求的最低密钥长度。

［解读］本条对强效加密的概念和密钥的有效长度进行定义。

随着计算机处理能力的不断提高，一些加密强度低的加密算法（DES、MD5 等）可以在短时间内被破解。因此，网上银行系统中使用的加密算法必须具有较高的抗破解能力。

3.9 资金类交易（Funds Transaction）

【原文】指通过网上银行进行资金操作交易，如转账、订单支付、缴费等。

本人名下的投资理财、托管账户以及本人签订委托代扣协议的委托代扣等风险可控的资金变动不属于此范畴。

［解读］本条对资金类交易的范围进行明确。

从广义上讲，涉及资金变化的交易都可以称做资金类交易。但在《规范》中，此定义细化为人为干预使资金发生变化的操作，而委托第三方使资金数额发生变化的不算做资金类交易。网上银行系统中的资金类交易脱胎于传统银行业务，它将银行柜台业务进行扩展，使交易更方便、更快捷。

3.10 信息及业务变更类交易（Information & Business Changing Transaction）

【原文】通过网上银行变更客户相关信息或开通、取消业务的交易，如客户修改基本信息、调整交易额度、授权委托交易、修改交易订单、开通（签订）新业务、取消某项业务、电子合同签署、电子保单等。

［解读］本条对信息及业务变更类交易的范围进行明确。

信息及变更类交易是指客户信息、客户变更业务范围等发生变化的交易。这些交易会涉及客户私人信息、资金额度等敏感数据，如果处理不当可能影响网上银行系统的安全性。

3.11 企业网银（Corporate Banking）

【原文】指商业银行等金融机构面向企事业单位和其他组织提供的网上金融服务。

［解读］本条对企业网银进行定义。

企业网银主要为企事业单位、组织机构提供网上银行服务，业务量较小但单笔交易金额较高。相比个人网银，企业网银提供更多针对企业的功能，应具有更高的安全级别。

4 符号和缩略语

为方便阅读，在对《规范》中的术语和定义进行解释后，本章节主要针对《规范》中使用的符号和缩略语进行解释，第5章、第6章中将大量使用这些符号和缩略语。

【原文】以下缩略语和符号表示适用于本标准：

CA	**数字证书签发和管理机构（Certification Authority）**
Cookies	**为辨别客户身份而储存在客户本地终端上的数据**
COS	**卡片操作系统（Card Operating System）**
C/S	**客户机/服务器（Client/Server）**
DoS/DDoS	**拒绝服务/分布式拒绝服务（Denial of Service/Distributed Denial of Service）**
IDS/IPS	**入侵检测系统/入侵防御系统（Intrusion Detection System/ Intrusion Prevention System）**
IPSEC	**IP 安全协议（Internet Protocol Security）**
OTP	**一次性密码（One Time Password）**
PKI	**公钥基础设施（Public Key Infrastructure）**
SSL	**安全套接字层（Secure Socket Layer）**
SPA/DPA	**简单能量分析/差分能量分析（Simple Power Analysis/ Differential Power Analysis）**
SEMA/DEMA	**简单电磁分析/差分电磁分析（Simple Electromagnetism Analysis/ Differential Electromagnetism Analysis）**
TLS	**传输层安全（Transport Layer Security）**
WTLS	**无线传输层安全（Wireless Transport Layer Security）**
VPN	**虚拟专用网络（Virtual Private Network）**
IMEI	**国际移动设备身份码（International Mobile Equipment Identity）**
IMSI	**国际移动用户识别码（International Mobile Subscriber Indentification Number）**