ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 20547.2—2006

银行业务　安全加密设备(零售)
第2部分:金融交易中设备安全符合性检测清单

Banking—Secure cryptographic devices (retail)—
Part 2: Security compliance checklists for devices used in financial transactions

(ISO 13491-2:2005,MOD)

2006-09-18 发布　　2007-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 20547.2—2006

中华人民共和国
国家标准
银行业务　安全加密设备(零售)
第2部分:金融交易中设备安全符合性检测清单
GB/T 20547.2—2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2　字数 53 千字
2007年3月第一版　2007年3月第一次印刷
*
书号:155066·1-29021　定价 24.00 元

GB/T 20547.2-2006

表 H.2(续)

序号	安全符合性声明	符合	不符合	不适用
H6	应保证： ——始终由至少两名已接受过培训的人员对设备进行持续监视，以确定设备是否被攻击或是否有其他人员接触设备。 ——通过摄像头以不低于 $x/2$ min 的频率监控或在设备附近有物体移动时对设备进行监视(通过安全的视频系统)，应有专人负责检查摄像设备是否有被攻击的迹象。 注："$x/2$ min"是"x 分钟"的一半，"x 分钟"是估算成功进行以下操作所需的时间。 ——对设备的硬件或者软件进行增加、替换或修改(如安装一个"偷窃"装置)。 ——探知或修改任何敏感信息(例如：个人识别码、访问代码和密钥)。然后在不需要特殊技能和特定工具情况下对设备重新安装，并且对设备造成的破坏不足以被察觉。 应注意摄像系统的安装，以保证不形成偷窥的可能性。			
H7	所有供人员或设备通过的出入口均应被持续监控，例如：设置保安人员职守。保安人员被要求除非有授权人员(搬运设备的人员除外)对设备进出签发的书面授权，否则不允许任何设备进出。			
H8	除通过受监控的出入口外，没有其他任何途径(如地板下或天花板上)可以不经授权地进入受控环境，或将设备移进/移出。			

H.5 安全环境

如表 H.3 所示，安全环境为不安全的设备提供了外部保护，并且明显比受控环境更加安全。安全环境可以是为达到此目的而设计的房间或安全室。无论采用什么形式，只有那些被授权访问设备的人才能够进入安全环境。安全环境经常设置在受控环境之中。

所有建立的安全程序应易于妥善归档管理与执行，审计师应定期核查这些程序并将核查结果提交审计机构。

表 H.3

序号	安全符合性声明	符合	不符合	不适用
H9	访问通过以下方式进行限制： ——入口处配置门锁并持续监视； ——成对的授权和可信人员； ——由成对的授权和可信人员陪同的人员。 未被监控的出入口应安装门锁并装有报警装置，任何进出这些出入口的行为都将受到保安人员的干预。			
H10	未经授权人员进入安全环境应由至少两名授权和可信人员陪同，并在安全环境中受到全程监督。			
H11	所有出入情况都应被记录，且该记录应安全保存并定期审查。			

目　　次

附　录　G
（规范性附录）
具有数字签名功能的设备

G.1　概述

数字签名设备生成或验证数字签名以提供数据完整性和真实性。在某些情况下，经过严格控制，数字签名也可以提供不可否认性。对数字签名生成来说，输入包括消息和私钥。对数字签名验证来说，输入包括消息和公钥。这两个功能的运算都是在安全加密设备(SCD)内完成的。

用来验证数字签名的公钥既不是秘密数据，也不是数字签名所保护的内容。但是，必须保证其完整性。

评估数字签名设备的过程如下：

——完成附录 A 中的检测清单；

——完成附录 E 中的检测清单；

——完成本附录中的检测清单；

——向审计机构提交上述评估结果。

下列安全符合性检测清单都要求审计师用“符合(T)”、“不符合(F)”和“不适用(N/A)”做出详细说明。“不符合”标记不表明该项在实际中不可接受，但应该给出书面解释。被标注为“不适用”的清单也应给出书面解释。

G.2　设备管理

G.2.1　基本要求

安全设备制造商和用户，以及要使用设备的个人或组织，都需要向审计机构提供如表 G.1 所示的保证。

表 G.1

序号	安全符合性声明	符合	不符合	不适用
G1	如果要求不可否认性，则： ——应在数字签名设备中生成非对称密钥对的私钥和公钥； ——不得以任何理由(包括备份和存档)从原始数字签名设备中输出非对称密钥对的私钥； ——建立控制私钥使用的机制。			

G.2.2　数字签名鉴别管理

由独立机构(内部或外部的)对数字签名设备的管理功能进行评估，并得出如表 G.2 所示的结论。

表 G.2

序号	安全符合性声明	符合	不符合	不适用
G2	为了便于审计和控制，应能通过以下方法关联公钥和私钥所有者： ——利用从一个授权认证机构得到的公钥证书； ——使用公钥证书和适当的证书管理程序； ——用其他类似机制来断定私钥拥有者的身份。			
G3	设备密钥管理功能遵守 ISO 11568 和国内相关法规的规定，特别是不允许签名密钥用于其他任何目的。			

前　言

GB/T 20547《银行业务　安全加密设备(零售)》分为如下部分：

——第 1 部分：概念、要求和评估方法

——第 2 部分：金融交易中设备安全符合性检测清单

本部分是 GB/T 20547 的第 2 部分。

本部分修改采用国际标准 ISO 13491-2:2005《银行业务 安全加密设备(零售)　第 2 部分：金融交易中设备安全符合性检测清单》(英文版)。

本部分对 ISO 13491-2:2005 所做的修改主要包括以下内容：

1. 将本部分中引用的国际标准改为国际标准和国内相关法规。

2. 删除目前国内不适用的部分规范性引用文件。

本部分的附录 A、附录 B、附录 C、附录 D、附录 E、附录 F、附录 G 和附录 H 为规范性附录。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会归口管理。

本部分起草单位：中国银联股份有限公司、中国人民银行、中国工商银行、中国银行股份有限公司、中国建设银行股份有限公司、交通银行、北京银联金卡科技有限公司。

本部分主要起草人：刘钟、孙平、黄发国、徐志忠、温永盛、陆书春、刘运、赵宏鑫、薛伟、张晓东、陈立群、钱菲、李曙光、刘志刚、任冠华、姜红、李洁。

本标准于 2006 年首次发布。