ICS 35.240.40
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0114—2015

网银系统 USBKey 规范 安全技术与测评要求

Specification for USBKey in internet banking system—
Security technique and evaluation requirements

2015 - 08 - 31 发布　　2015 - 08 - 31 实施

中国人民银行　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准主要起草单位：中国信息安全测评中心、中国工商银行股份有限公司、中国金融电子化公司、北京博时信力科技有限公司、飞天诚信科技股份有限公司、天地融科技股份有限公司。

本标准参与起草单位：银行卡检测中心、国家信息技术安全研究中心。

本标准主要起草人：张翀斌、高金萍、杨永生、石竑松、郭颖、王贵智、曾凯、刘鹞、王昱、朱鹏飞、李明、赵乔伟、安焘、李冰、贾嘉。

网银系统 USBKey 规范 安全技术与测评要求

1 范围

本标准规定了网银系统USBKey的安全技术要求及对网银系统USBKey进行测评的相关要求和方法。

本标准适用于网银系统USBKey的研发、测试、评估和产品采购。

通常所说的一代USBKey由于不符合硬件要求，故不适用于本标准。

2 规范性引用文件

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 18336 信息技术 安全技术 信息技术安全性评估准则

GB/T 22186 信息安全技术 具有中央处理器的集成电路（IC）卡芯片安全技术要求（评估保证级4增强级）

JR/T 0068 网上银行系统信息安全通用规范

JR/T 0098.2 中国金融移动支付 检测规范 第2部分：安全芯片

3 术语和定义

GB/T 18336界定的以及下列术语和定义适用于本文件。

3.1

个人化数据 personalization data

网银系统USBKey在个人化阶段写入的个性化数据。

3.2

集成电路芯片 integrated circuit chip

网银系统USBKey的核心硬件，具有运算处理能力，是相关软件运行的平台。

3.3

签名 signature

使用用户的私钥对交易相关数据实施数字签名操作。

3.4

状态机 state machine

网银系统USBKey运行时，应维护相应的状态，以保障操作在相应状态允许下才可执行。

3.5

用户 user

使用网银系统USBKey的操作人员。

3.6

管理员 administrator

对网银系统USBKey实施个人化、初始化、解锁等管理操作的人员。

3.7

中间件 middle ware

提供软件接口的程序，存储在PC机或移动终端等计算设备中，可根据传入的参数，向USBKey下发指令或指令序列，接收USBKey回送的数据，并向调用方报告指令执行情况。

3.8

个人识别码 personal identification number（PIN）

用于鉴别USBKey用户身份，防止其功能被未授权使用的一串字符序列。

注：在用户使用USBKey进行某些敏感操作前（如交易签名），USBKey需要验证用户是否知道该字符序列。

4 缩略语

下列缩略语适用于本文件。

TOE：评估对象（Target of Evaluation）

TSF：TOE安全功能（TOE Security Functions）

EAL：评估保证级（Evaluation Assurance Level）

TSP：TOE安全策略(TOE Security Policy)

CM：配置管理（Configuration Management）

CSP：密码服务提供者(Cryptographic Service Provider)

PKCS：公钥密码标准(Public-Key Cryptography Standards)

5 网银系统 USBKey 描述

5.1 概述

网银系统USBKey是服务于金融交易业务，内置集成电路芯片，具有一定的存储空间，可以存储用户的私钥以及数字证书，实现对关键金融交易数据实施数字签名功能的设备。

本标准所指的TOE即网银系统USBKey，包括USBKey自身的软件、硬件，以及与系统应用交互的中间件，如图1中的虚线框所示范围，可通过C/S或B/S模式与银行网银系统进行交互。

网银系统USBKey除配备按键及显示屏功能外，还可附加语音提示、语音识别等其他功能。同时，网银系统USBKey的通信接口不局限于USB接口，采用蓝牙、音频等其他接口形式的产品也适用于本标准。

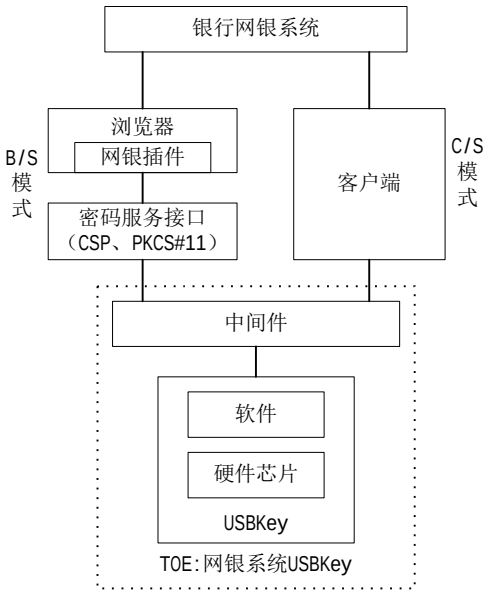

图1　网银系统 USBKey 一般框架图

5.2　生命周期

网银系统USBKey生命周期可分为以下几个阶段，各个阶段内容如表1所示。

表1　网银系统 USBKey 产品的生命周期

阶段	内容
阶段 1 开发阶段	硬件设计，软件开发
阶段 2 生产制造阶段	网银系统 USBKey 制造，软件加载
阶段 3 应用初始阶段	配置相应数据，在安全的环境中完成 USBKey 的应用初始化、个人化
阶段 4 使用阶段	将 USBKey 交付给最终用户，供用户使用
阶段 5 废止阶段	USBKey 废弃后，不得在网银系统中继续使用

6　安全环境

6.1　概述

本章描述网银系统USBKey的预期使用环境及使用方式，包括网银系统USBKey需要保护的信息和资源、有关网银系统USBKey应用环境的说明、对资产的威胁及网银系统USBKey应用应遵循的组织安全策略等内容。

6.2　资产

网银系统USBKey需要保护以下资产：

——TSF数据（如TOE生命周期状态、安全状态、密钥、PIN、数字证书、配置数据、文件系统等信息）。

——用户数据（TOE中不属于TSF数据的信息，如交易数据、字库信息等）。

——数字签名能力（仅限于合法用户能使用存储的私钥进行数字签名的能力）。

6.3 应用环境说明

6.3.1 人员

假设操作USBKey人员已具备基本的安全防护知识并具有良好的使用习惯，可确保以安全的方式使用USBKey。

6.3.2 管理

假设对USBKey进行个人化、初始化的管理者无恶意，并按照相关规定进行管理操作，可确保USBKey中的关键数据不被泄露。

6.4 网银系统 USBKey 面临的威胁

6.4.1 签名伪造

攻击者可能利用密钥管理系统或密码算法及实现的缺陷，冒充USBKey的合法用户进行有效的数字签名。

6.4.2 未授权使用

攻击者在未授权的情况下可能利用USBKey执行非法操作，如未经身份验证执行签名、利用社会工程等方法诱导用户偏离安全操作流程，通过木马等恶意软件远程操控USBKey，或USBKey丢失后被别人使用。

6.4.3 交互数据监听

攻击者可能通过监听用户与USBKey之间的交互过程，以获取可用数据信息。

6.4.4 交互数据篡改

攻击者可能修改用户与USBKey之间的交互数据，以获得操作USBKey的权限或伪造数字签名。

6.4.5 敏感数据遍历

攻击者可能利用对数据空间的反复搜索或重复操作，来获取重要安全数据信息。如对PIN码和密钥的穷举攻击。

6.4.6 重放攻击

攻击者可能通过重放通信数据，获取操作权限或伪造虚假交易过程等，如重放监听获得的PIN验证数据，以绕过安全机制等。

6.4.7 审计数据篡改

攻击者可能通过修改或删除相关审计信息，来获取相应的安全权限或改变网银系统USBKey的关键安全要素。

6.4.8 数据访问控制机制旁路

攻击者可能绕过文件等数据的访问控制机制，以获取或篡改网银系统USBKey的敏感数据信息。

6.4.9 生命周期功能滥用

攻击者可能会利用与USBKey当前生命周期阶段不相关的命令，尤其是测试和调试命令、初始化命令等，以读取或修改网银系统USBKey安全功能或敏感数据信息。

6.4.10 安全状态扰乱

攻击者可能在使用过程中实施非正常操作，如未经PIN验证执行签名、恶意插入指令、重组指令、断电、取消操作、操作超时、按键持续导通、未经按键确认读取签名等，以扰乱USBkey的安全机制或破坏其安全环境，使USBKey进入不安全状态导致功能异常。

6.4.11 侧信道攻击

攻击者可能对网银系统USBKey操作过程中的功耗、电磁辐射等侧信道信息进行分析，以获得USBKey的敏感数据信息。

6.4.12 差错注入攻击

攻击者可能采用错误注入的方法，破坏USBKey的功能或获得其敏感数据信息。如光攻击，电压毛刺注入、电磁操纵等错误注入方法。

6.4.13 物理操纵

攻击者可利用USBKey芯片失效性分析和半导体逆向工程技术，对芯片实施物理剖片，以获取芯片设计信息和嵌入式软件代码，进而探测TSF数据和用户数据信息。攻击者也可能对芯片实施物理更改，以达到获取、改变数据信息或安全功能的目的。

6.4.14 环境压力

攻击者可能采用改变外界环境条件的方法，破坏USBKey的功能或获得其敏感数据信息。如改变运行温度、工作电压、工作频率等方法。

6.4.15 中间件信息泄露

攻击者可能对中间件实施逆向分析或PIN码输入截取等攻击，以获取其保存的用户数据或密钥等敏感数据信息。

6.4.16 中间件功能篡改

攻击者可能篡改或替换中间件及USBKey的驱动程序，以旁路中间件相关的安全功能。

6.5 组织安全策略

6.5.1 密码算法

密码算法的使用应符合国家密码主管部门的要求。

6.5.2 标识

网银系统USBKey应具备唯一标识。

6.5.3 芯片

网银系统USBKey的芯片应满足EAL4+保证级及AVA.VLA.4的要求。

7 安全目的

7.1 概述

针对第6章提出的网银系统USBKey需要满足的安全需求，本章以安全目的的形式明确界定网银系统USBKey技术措施满足的安全需求，以及由网银系统USBKey环境（即非IT手段）来满足的安全需求。

7.2 TOE 安全目的

7.2.1 签名防伪造

网银系统USBKey应采用安全的设计及实现方法，以防止用户的签名被伪造。

7.2.2 密码支持

网银系统USBKey应以安全的方式支持密码功能和随机数生成功能。

7.2.3 使用授权

网银系统USBKey应以安全的方式管理用户数据和相关应用，防止其被未授权的用户使用。USBKey应提供相应的功能防止攻击者劫持USBKey并利用其功能。

7.2.4 安全通信

在TOE内部传输TSF数据时，网银系统USBKey应提供一种处理机制以保证数据传输的安全性，即真实性和完整性，以防止敏感数据泄露或被篡改。

7.2.5 防数据遍历

网银系统USBKey应抵御未授权实体对网银系统USBKey中的数据遍历攻击，如对口令的搜索。

7.2.6 防数据重放

网银系统USBKey应提供安全机制，如加入随机因子等，以抵御数据重放攻击。

7.2.7 审计

网银系统USBKey应能提供安全审计手段，记录选定的审计信息，以便确定网银系统USBKey是否响应相关操作。

7.2.8 数据保护

网银系统USBKey应提供安全机制，防止数据被非法访问、删除或修改。如在使用阶段应禁止对主文件的删除或重建。

7.2.9 生命周期控制功能

在网银系统USBKey的特定生命周期阶段有效的专有命令，在其他阶段应该被禁止，以保证指令集在可控的范围内。

7.2.10 访问控制

网银系统USBKey应制定严格的访问控制策略以防止非法使用网银系统USBKey的相关功能。

7.2.11 指令流程保护

网银系统USBKey的关键操作流程应有严格的指令执行顺序，防止指令间的相互干扰而影响操作结果。

7.2.12 安全状态维护

网银系统USBKey应能维护相关安全状态，如PIN安全状态、按键状态，使其在安全策略内执行安全操作。

7.2.13 掉电保护

在写操作过程中发生掉电故障时，网银系统USBKey应确保数据的正确性和可用性，使得USBKey在重新加电后可进入安全的工作状态。

7.2.14 防侧信道攻击

USBKey应具备抵抗侧信道攻击的能力，以防止通过能量、电磁变化等侧信道信息泄露密钥等敏感信息。

7.2.15 防差错注入攻击

USBKey应具备抵抗差错注入攻击的能力，以防止泄露机密数据或安全功能失常。

7.2.16 防环境扰动攻击

USBKey在外界环境条件改变的情况下，应采取有效保护措施，以防止泄露机密数据或安全功能失常。

7.2.17 中间件程序保护

USBKey的中间件程序提供自我保护机制，提供抗反汇编、抗逆向分析等保护措施，防止攻击者对程序的调试，分析和篡改，或防止USBKey驱动被篡改或替换。

USBKey的中间件程序应提供处理措施，以防止恶意程序获取或篡改中间件的敏感信息，如获取PIN码信息，密钥信息等。

7.2.18 标识

网银系统USBKey应能记录并保存能够唯一识别其自身的标识信息。

7.2.19 角色管理

网银系统USBKey应能对用户和管理员角色进行管理。

7.3 环境安全目的

7.3.1 人员安全

USBKey操作人员应具备基本的安全防护知识并具有良好的使用习惯，可确保USBKey的运行环境满足安全要求，且用户以正确的方式使用USBKey。

7.3.2 管理安全

对网银系统USBKey进行个人化、初始化、注销废止的管理者应无恶意，并按照相关规定进行管理操作，确保USBKey中的关键数据不被泄露，并使同一型号USBKey在不同银行的网上银行系统中应用时，使用不同的根密钥产生其他相关子密钥。

7.3.3 密码算法安全

密码算法的使用应符合国家密码主管部门的要求。

7.3.4 芯片安全

网银系统USBKey的芯片应满足EAL4+保证级及AVA.VLA.4的要求，以抵抗针对芯片的侧信道、差错注入、物理探测与修改等形式的侵入式、半侵入式或非侵入式物理攻击。

注：侵入式、半侵入式或非侵入式攻击具体内容可参见JR/T 0098.2。

8 安全要求

8.1 概述

针对第 7 章提出的安全目的，本章提出网银系统 USBKey 安全目的的安全功能和安全保证要求。

表2列出网银系统USBKey安全功能要求组件，表3列出网银系统USBKey需满足的安全保证要求组件。

表 2 安全功能要求组件

安全功能要求组件	组件名称
FAU_GEN.1	审计数据产生
FAU_STG.1	受保护的审计迹存储
FCS_CKM.1	密钥生成
FCS_CKM.3	密钥存取
FCS_CKM.4	密钥销毁
FCS_COP.1	密码运算
FCS_RNG.1	随机数生成
FDP_ACC.1	子集访问控制
FDP_ACF.1	基于安全属性的访问控制
FDP_RIP.1	子集残余信息保护
FDP_ROL.1	基本回退
FIA_AFL.1	鉴别失败处理
FIA_UAU.1	鉴别的时机
FIA_UAU.4	一次性鉴别机制
FIA_UAU.5	多重鉴别机制
FIA_UID.1	标识的时机
FMT_MOF.1	安全功能行为的管理
FMT_MTD.1	安全功能数据的管理
FMT_SMF.1	管理功能规范
FMT_SMR.1	安全角色

表 2 （续）

安全功能要求组件	组件名称
FPT_PHP.3	物理攻击抵抗
FPT_RCV.4	功能恢复
FPT_RPL.1	重放检测
FPT_ITT.1	内部 TSF 数据传送的基本保护
FTA_SSL.3	原发会话终止

表 3 安全保证要求组件

安全保证要求组件	组件名称
ACM_CAP.3	授权控制
ACM_SCP.1	TOE CM 覆盖
ADO_DEL.1	交付程序
ADO_IGS.1	安装、生成和启动程序
ADV_FSP.1	非形式化功能规范
ADV_HLD.2	安全加强的高层设计
ADV_RCR.1	非形式化对应性证实
AGD_ADM.1	管理者指南
AGD_USR.1	用户指南
ALC_DVS.1	安全措施标识
ATE_COV.2	覆盖分析
ATE_DPT.1	测试：高层设计
ATE_FUN.1	功能测试
ATE_IND.2	独立测试—抽样
AVA_MSU.1	指南审查
AVA_SOF.1	TOE 安全功能强度评估
AVA_VLA.4	高级抵抗力

8.2 安全功能要求

8.2.1 审计数据产生（FAU_GEN.1）

FAU_GEN.1.1 网银系统 USBKey 的安全功能应能为 USBKey 唯一标识信息生成审计记录。

8.2.2 受保护的审计迹存储（FAU_STG.1）

FAU_STG.1.1 网银系统 USBKey 安全功能应保护所存储的审计记录，以避免未授权的删除。

FAU_STG.1.2 网银系统 USBKey 安全功能应能防止对审计记录的未授权修改。

8.2.3 密钥生成（FCS_CKM.1）

FCS_CKM.1.1 网银系统 USBKey 安全功能应根据网银系统应用要求在 USBKey 内部产生密钥长度为【2048bits，***赋值：其他密钥长度***】的【**非对称密钥加密算法** RSA，***赋值：符合国家密码主管部门要求的其他算法***】的密钥。禁止向 USBKey 写入私钥、不固化密钥

对和用于生成密钥对的素数。

8.2.4 密钥存取（FCS_CKM.3）

FCS_CKM.3.1 网银系统 USBKey 安全功能应根据网银系统应用要求，执行除公钥之外的任何密钥不得输出的密钥访问方法，且以安全方式存储、更新密钥。

8.2.5 密钥销毁（FCS_CKM.4）

FCS_CKM.4.1 应根据网银系统应用要求，采用**【新密钥覆盖旧密钥的方法，*赋值：其他密钥销毁方法*】**来销毁交易签名算法相关密钥。

8.2.6 密码运算（FCS_COP.1）

FCS_COP.1.1 （1）网银系统 USBKey 安全功能应根据网银系统应用要求来执行密钥长度为**【64bits 和 128bits，*赋值：其他密钥长度*】**的**【对称密钥加密算法 DES 和 TDES，*赋值：符合国家密码主管部门要求的其他算法*】**运算。

FCS_COP.1.1 （2）网银系统 USBKey 安全功能应根据网银系统应用要求来执行密钥长度为**【2048bits，*赋值：其他密钥长度*】**的**【非对称密钥加密算法 RSA，*赋值：符合国家密码主管部门要求的其他算法*】**运算。

FCS_COP.1.1 （3）网银系统 USBKey 安全功能应根据网银系统应用要求来执行**【Hash 算法 SHA-1，*赋值：符合国家密码主管部门要求的其他算法*】**运算。

FCS_COP.1.1（4)网银系统 USBKey 安全功能应根据网银系统应用要求来执行密钥长度为**【112bits，*赋值：符合国家密码主管部门要求的其他密钥长度*】**的**【MAC 操作，*赋值：其他算法*】**运算。

8.2.7 随机数生成（FCS_RNG.1）

FCS_RNG.1.1 网银系统USBKey安全功能将具有随机数生成功能。

FCS_RNG.1.2 网银系统USBKey所生成的随机数应符合国际通用标准要求的特定随机数质量要求。

8.2.8 子集访问控制（FDP_ACC.1）

FDP_ACC.1.1 （1）网银系统 USBKey 安全功能将对**【主体：用户，客体：交易数据，它们之间的操作：签名】**执行**【交易签名访问控制策略】**。

FDP_ACC.1.1 （2）网银系统 USBKey 安全功能将对**【主体：用户，客体：签名公私钥，它们之间的操作：生成、删除】**执行**【签名公私钥访问控制策略】**。

8.2.9 基于安全属性的访问控制（FDP_ACF.1）

FDP_ACF.1.1 （1）网银系统 USBKey 安全功能将基于用户鉴别状态对客体执行交易签名访问控制策略。

FDP_ACF.1.1 （2）网银系统 USBKey 安全功能将基于用户鉴别状态对客体执行签名公私钥访问控制策略。

FDP_ACF.1.2 （1）网银系统 USBKey 安全功能将基于**【PIN 验证通过，按键确认，*赋值：或其他验证方式*】**授权主体访问客体，并在 USBKey 上以明确的方式提示用户。

FDP_ACF.1.2 （2）网银系统 USBKey 安全功能将基于**【PIN 验证通过，按键确认，*赋值：或其他验证方式*】**授权主体访问客体，并在 USBKey 上以明确的方式提示用户。

8.2.10 子集残余信息保护（FDP_RIP.1）

FDP_RIP.1.1（1）网银系统 USBKey 安全功能应确保在【生成新的交易签名密钥对后，USBKey 非易失性存储器中存储的旧密钥对】不可再用。

FDP_RIP.1.1（2）网银系统 USBKey 安全功能应确保在【使用完交易签名密钥对和 PIN 后，USBKey 会及时清除 RAM 中存储的密钥对和 PIN】，使其不可再用。

FDP_RIP.1.1（3）网银系统 USBKey 安全功能应确保在【使用完 PIN 后，网银系统 USBKey 中间件会及时清除其存储的 PIN】，使其不可再用。

8.2.11 基本回退（FDP_ROL.1）

FDP_ROL.1.1 网银系统 USBKey 安全功能应在【**签名数据格式错误、签名流程被破坏、签名成功、签名取消操作、签名超时的条件，*赋值：其他安全操作***】下进行【**安全状态，如 PIN 码及相关数据内容等**】的回退操作。复位安全状态，防止签名数据在最终确认前被替换，并在 USBKey 上以明确的方式提示用户。

8.2.12 鉴别失败处理（FIA_AFL.1）

FIA_AFL.1.1 网银系统 USBKey 安全功能应能检测并记录 PIN 验证相关的剩余鉴别尝试的次数。

FIA_AFL.1.2 （1）当 PIN 鉴别尝试次数还有 2 次时，网银系统 USBKey 安全功能将采取提示用户确认该鉴别操作。

FIA_AFL.1.2 （2）当 PIN 码验证失败时，USBKey 应进入安全状态，且当 PIN 鉴别连续失败次数达到上限时（不超过 10 次），网银系统 USBKey 安全功能应锁定 PIN。

8.2.13 鉴别的时机（FIA_UAU.1）

FIA_UAU.1.1 在用户被鉴别前，用户可执行【**除交易数据签名、密钥对生成、*赋值：其他金融安全操作之外的操作，如读取 USBKey 基本信息等操作***】。

8.2.14 一次性鉴别机制（FIA_UAU.4）

FIA_UAU.4.1 网银系统 USBKey 安全功能应防止与 PIN 验证鉴别机制有关的鉴别数据的再次使用，如采用随机数参与 PIN 鉴别过程来防止重放。

8.2.15 多重鉴别机制（FIA_UAU.5）

FIA_UAU.5.1 网银系统 USBKey 应提供【**PIN 验证、按键确认的鉴别机制，*赋值：其他鉴别机制***】以支持用户鉴别。

FIA_UAU.5.2 网银系统 USBKey 应根据【**用户输入 PIN 值正确与否及执行按键确认操作与否，*赋值：其他鉴别机制通过与否***】鉴别交易签名用户所声称的身份。

8.2.16 标识的时机（FIA_UID.1）

FIA_UID.1.1 在用户被标识前，用户可执行除交易数据签名和密钥对生成之外的其他基本操作，如读取 USBKey 基本信息等操作。

8.2.17 安全功能行为的管理（FMT_MOF.1）

FMT_MOF.1.1 网银系统 USBKey 安全功能应仅限于管理员具有解锁 PIN 和初始化 USBKey 的权力。

8.2.18 安全功能数据的管理（FMT_MTD.1）

FMT_MTD.1.1 （1）网银系统 USBKey 安全功能应仅限于管理员能够对 PIN 值、PIN 验证失败次数进行重置操作。

FMT_MTD.1.1 （2）网银系统 USBKey 安全功能应仅限于授权用户能够对 PIN 值进行修改操作。

FMT_MTD.1.1 （3）网银系统 USBKey 安全功能应仅限于管理员能够对 USBKey 中存储的相关维护密钥进行修改操作。

FMT_MTD.1.1 （4）网银系统 USBKey 安全功能应以安全方式存储安全数据（如 PIN、密钥）。

8.2.19 管理功能规范（FMT_SMF.1）

FMT_SMF.1.1 网银系统 USBKey 安全功能应能够执行如下安全管理功能：对应用初始、使用配置等生命周期进行控制管理，防止非本生命周期阶段内的功能被滥用。如，用户阶段应禁止对主文件的删除和重建操作。

8.2.20 安全角色（FMT_SMR.1）

FMT_SMR.1.1 网银系统 USBKey 安全功能应维护授权用户和管理员角色。

FMT_SMR.1.2 网银系统 USBKey 安全功能应能够把用户和角色关联起来。

8.2.21 物理攻击抵抗（FPT_PHP.3）

FPT_PHP.3.1 网银系统 USBKey 安全功能应能抵抗对【网银系统 USBKey 安全功能】的【中间件逆向分析，及芯片的侵入式、半侵入式及非侵入式攻击】。

注：对芯片的侵入式、半侵入式及非侵入式攻击参见JR/T 0098.2。

8.2.22 功能恢复（FPT_RCV.4）

FPT_RCV.4.1 （1）网银系统 USBKey 应确保掉电发生时，相关的生成密钥对、PIN 验证、PIN 修改操作或者成功完成，或者出现指明的失败情况后，应恢复到一个安全状态。

FPT_RCV.4.1 （2）网银系统 USBKey 应确保按键持续导通时，按键确认操作将不能成功完成，应恢复到一个安全状态。

8.2.23 重放检测（FPT_RPL.1）

FPT_RPL.1.1 网银系统 USBKey 安全功能应检测 PIN 验证数据、PIN 修改数据、USBKey 屏显的签名交易数据的重放。

FPT_RPL.1.2 检测到重放时，网银系统 USBKey 应执行**【拒绝操作并复位安全状态，*赋值：其他安全操作*】**。

8.2.24 内部 TSF 数据传送的基本保护（FPT_ITT.1）

FPT_ITT.1.1 网银系统 USBKey 安全功能应保护 TSF 数据（如 PIN、密钥等）在 TOE 内部传输时不被泄露和修改。

8.2.25 原发会话终止（FTA_SSL.3）

FTA_SSL.3.1 网银系统USBKey安全功能应在一段时间无任何操作，或需用户按键确认操作的等待时间超过3分钟之后终止交互式会话，并通过语音或屏幕显示提醒告知用户。

8.3 安全保证要求

8.3.1 授权控制（ACM_CAP.3）

开发者行为元素：

ACM_CAP.3.1D 开发者应为 TOE 提供一个参照号。

ACM_CAP.3.2D 开发者应使用一个 CM 系统。

ACM_CAP.3.3D 开发者应提供 CM 文档。

证据的内容和形式元素：

ACM_CAP.3.1C TOE 参照号对 TOE 的每一个版本应是唯一的。

ACM_CAP.3.2C 应给 TOE 标记上参照号。

ACM_CAP.3.3C CM 文档应包括一个配置清单和一个 CM 计划。

ACM_CAP.3.4C 配置清单应唯一标识组成 TOE 的所有配置项。

ACM_CAP.3.5C 配置清单应描述组成 TOE 的配置项。

ACM_CAP.3.6C CM 文档应描述用于唯一标识 TOE 所包含配置项的方法。

ACM_CAP.3.7C CM 系统应唯一标识 TOE 所包含的所有配置项。

ACM_CAP.3.8C CM 计划应描述 CM 系统是如何使用的。

ACM_CAP.3.9C 证据应证实 CM 系统的运行与 CM 计划是一致的。

ACM_CAP.3.10C CM 文档应提供所有配置项都已经和正在 CM 系统下有效地进行维护的证据。

ACM_CAP.3.11C CM 系统应提供措施使得只能对配置项进行授权改变。

8.3.2 TOE CM 覆盖（ACM_SCP.1）

开发者行为元素：

ACM_SCP.1.1D 开发者应提供一个 TOE 配置项列表。

证据的内容和形式元素：

ACM_SCP.1.1C 配置项列表应包括：实现表示和 ST 中其他保证组件所要求的评估证据。

8.3.3 交付程序（ADO_DEL.1）

开发者行为元素：

ADO_DEL.1.1D 开发者应将把 TOE 或其部分交付给用户的程序文档化。

ADO_DEL.1.2D 开发者应使用交付程序。

证据的内容和形式元素：

ADO_DEL.1.1C 交付文档应描述，在向用户方分发 TOE 版本时，用以维护其安全性所必需的所有程序。

8.3.4 安装、生成和启动程序（ADO_IGS.1）

开发者行为元素：

ADO_IGS.1.1D 开发者应将 TOE 安全地安装、生成和启动必需的程序文档化。

证据的内容和形式元素：

ADO_IGS.1.1C 安装、生成和启动文档应描述 TOE 安全地安装、生成和启动必需的所有步骤。

8.3.5 非形式化功能规范（ADV_FSP.1）

开发者行为元素：

ADV_FSP.1.1D 开发者应提供一个功能规范。

证据的内容和形式元素：

ADV_FSP.1.1C 功能规范应使用非形式化风格来描述 TSF 及其外部接口。

ADV_FSP.1.2C 功能规范应是内在一致的。

ADV_FSP.1.3C 功能规范应描述所有外部 TSF 接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节。

ADV_FSP.1.4C 功能规范应完备地表示 TSF。

8.3.6 安全加强的高层设计（ADV_HLD.2）

开发者行为元素：

ADV_HLD.2.1D 开发者应提供 TSF 的高层设计。

证据的内容和形式元素：

ADV_HLD.2.1C 高层设计的表示应是非形式化的。

ADV_HLD.2.2C 高层设计应是内在一致的。

ADV_HLD.2.3C 高层设计应按子系统描述 TSF 的结构。

ADV_HLD.2.4C 高层设计应描述每个 TSF 子系统所提供的安全功能性。

ADV_HLD.2.5C 高层设计应标识 TSF 所要求的任何基础性硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示。

ADV_HLD.2.6C 高层设计应标识 TSF 子系统的所有接口。

ADV_HLD.2.7C 高层设计应标识 TSF 子系统的哪些接口是外部可见的。

ADV_HLD.2.8C 高层设计应描述 TSF 子系统所有接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节。

ADV_HLD.2.9C 高层设计应把 TOE 分成 TSP-实施和其他子系统来描述。

8.3.7 非形式化对应性证实（ADV_RCR.1）

开发者行为元素：

ADV_RCR.1.1D 开发者应提供一个所提供 TSF 表示的所有相邻对之间对应性的分析。

证据的内容和形式元素：

ADV_RCR.1.1C 对于所提供 TSF 表示的每个相邻对，分析应证实，较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

8.3.8 管理员指南（AGD_ADM.1）

开发者行为元素：

AGD_ADM.1.1D 开发者应提供针对系统管理员的管理员指南。

证据的内容和形式元素：

AGD_ADM.1.1C 管理员指南应描述 TOE 管理员可使用的管理功能和接口。

AGD_ADM.1.2C 管理员指南应描述如何以安全的方式管理 TOE。

AGD_ADM.1.3C 管理员指南应包含一些关于安全处理环境中应被控制的功能和特权的警示信息。

AGD_ADM.1.4C 管理员指南应描述所有关于与 TOE 安全运行有关用户行为的假设。

AGD_ADM.1.5C 管理员指南应描述所有受管理员控制的安全参数，适当时应指明安全值。

AGD_ADM.1.6C 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件，包括改变 TSF 所控制实体的安全特性。

AGD_ADM.1.7C 管理员指南应与供评估的所有其他文档保持一致。

AGD_ADM.1.8C 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

8.3.9 用户指南（AGD_USR.1）

开发者行为元素：

AGD_USR.1.1D 开发者应提供用户指南。

证据的内容和形式元素：

AGD_USR.1.1C 用户指南应描述 TOE 的非管理员用户可使用的功能和接口。

AGD_USR.1.2C 用户指南应描述 TOE 所提供的用户可访问安全功能的使用。

AGD_USR.1.3C 用户指南应包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息。

AGD_USR.1.4C 用户指南应清晰地阐述 TOE 安全运行所必需的所有用户职责，包括与 TOE 安全环境陈述中可找到的与关于用户行为的假设有关的那些职责。

AGD_USR.1.5C 用户指南应与供评估的所有其他文档保持一致。

AGD_USR.1.6C 用户指南应描述所有与用户有关的 IT 环境安全要求。

8.3.10 安全措施标识（ALC_DVS.1）

开发者行为元素：

ALC_DVS.1.1D 开发者应提供开发安全文档。

证据的内容和形式元素：

ALC_DVS.1.1C 开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

ALC_DVS.1.2C 开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据。

8.3.11 覆盖分析（ATE_COV.2）

开发者行为元素：

ATE_COV.2.1D 开发者应提供测试覆盖的一个分析。

证据的内容和形式元素：

ATE_COV.1.1C 测试覆盖的分析应证实测试文档中所标识的测试与功能规范中所描述的 TSF 之间的对应性。

ATE_COV.2.2C 测试覆盖的分析应证实功能规范中所描述 TSF 与测试文档所标识的测试之间的对应性是完备的。

8.3.12 测试：高层设计（ATE_DPT.1）

开发者行为元素：

ATE_DPT.1.1D 开发者应提供测试深度的分析。

证据的内容和形式元素：

ATE_DPT.1.1C 深度分析应证实测试文档中所标识的测试足以证实该 TSF 是依照其高层设计运行的。

8.3.13 功能测试（ATE_FUN.1）

开发者行为元素：

ATE_FUN.1.1D 开发者应测试 TSF，并文档化测试结果。

ATE_FUN.1.2D 开发者应提供测试文档。

证据的内容和形式元素：

ATE_FUN.1.1C 测试文档应包括测试计划、测试程序描述、预期的测试结果和实际的测试结果。

ATE_FUN.1.2C 测试计划应标识要测试的安全功能和描述要执行的测试的目标。

ATE_FUN.1.3C 测试程序描述应标识要执行的测试和描述每个安全功能的测试脚本。这些脚本应包

括对于其他测试结果的任何顺序依赖性。

ATE_FUN.1.4C 预期的测试结果应指出测试成功执行后的预期输出。

ATE_FUN.1.5C 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

8.3.14 独立测试—抽样（ATE_IND.2）

开发者行为元素：

ATE_IND.2.1D 开发者应提供用于测试的 TOE。

证据的内容和形式元素：

ATE_IND.2.1C TOE 应适合测试。

ATE_IND.2.2C 开发者应提供一组相当的资源，用于开发者的 TSF 功能测试。

8.3.15 指南审查(AVA_MSU.1)

开发者行为元素：

AVA_MSU.1.1D 开发者应提供指导性文档。

证据的内容和形式元素：

AVA_MSU.1.1C 指导性文档应标识所有可能的 TOE 运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义。

AVA_MSU.1.2C 指导性文档应是完备的、清晰的、一致的、合理的。

AVA_MSU.1.3C 指导性文档应列出关于预期使用环境的所有假设。

AVA_MSU.1.4C 指导性文档应列出对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

8.3.16 TOE 安全功能强度评估(AVA_SOF.1)

开发者行为元素：

AVA_SOF.1.1D 开发者应对 ST 中所标识的每个具有 TOE 安全功能强度声明的安全机制进行 TOE 安全功能强度分析。

证据的内容和形式元素：

AVA_SOF.1.1C 对于每个具有 TOE 安全功能强度声明的安全机制，TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的最低强度级别。

AVA_SOF.1.2C 对于每个具有特定 TOE 安全功能强度声明的安全机制，TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的特定功能强度度量。

8.3.17 高级抵抗力（AVA_VLA.4）

开发者行为元素：

AVA_VLA.4.1D 开发者应执行脆弱性分析。

AVA_VLA.4.2D 开发者应提供脆弱性分析文档。

证据的内容和形式元素：

AVA_VLA.4.1C 脆弱性分析文档应描述为搜索用户能违反 TSP 的方法而执行的 TOE 可交付材料分析，违反 TSP 的方法应包括 6.4 条中列出的所有威胁可利用的脆弱性。

AVA_VLA.4.2C 脆弱性分析文档应描述对已标识的脆弱性的处置。

AVA_VLA.4.3C 脆弱性分析文档应针对所有已标识的脆弱性，说明脆弱性不能在 TOE 的预期使用环境中被利用。

AVA_VLA.4.4C 脆弱性分析文档应证明存在已标识脆弱性的 TOE 可以抵御明显的穿透性攻击。
AVA_VLA.4.5C 证据应说明对脆弱性的搜索是系统化的。
AVA_VLA.4.6C 脆弱性分析文档应提供分析完备地处理了 TOE 可交付材料的证明材料。

9 测评要求

9.1 概述

针对第8章提出的安全要求，本章提出网银系统USBKey的测评要求和方法。

9.2 安全功能要求测评要求

9.2.1 审计数据产生（FAU_GEN.1）

测评目的：
验证网银系统USBKey的审计功能。
测评内容：
网银系统USBKey是否记录USBKey唯一标识信息。
测评方法：
通过指令读取USBKey标识信息并确认其是否可唯一标识USBKey。

9.2.2 受保护的审计迹存储（FAU_STG.1）

测评目的：
验证网银系统USBKey对所存储审计记录的保护功能。
测评内容：
网银系统USBKey是否可防止对USBKey唯一标识信息的未授权修改。
测评方法：
通过调用相关指令等方法修改USBKey唯一标识信息确认其是否可被修改。

9.2.3 密钥生成（FCS_CKM.1）

测评目的：
验证网银系统USBKey非对称密码算法相关密钥的生成功能。
测评内容：
网银系统USBKey是否能正确实现非对称密码算法的公私钥对生成功能。
测评方法：

a) 通过指令生成 RSA 算法 2048bits 公私钥对，并通过源代码验证其是否采用了安全的方式生成，并确认 RSA 算法未固化密钥对和用于生成密钥对的素数；
b) 利用生成的密钥对执行相关加解密操作，以验证其正确性；
c) 若网银系统 USBKey 开发者使用其他非对称密码算法，可按其特定密钥长度及算法特性进行验证。

9.2.4 密钥存取（FCS_CKM.3）

测评目的：
验证网银系统USBKey对存储的密钥的访问控制功能。
测评内容：

网银系统USBKey是否使用安全的方式来存取密钥。

测评方法：

通过指令读取、分析设计文档等方法分析网银系统USBKey中存储的密钥，确认除公钥之外的任何密钥不能被读出，并分析密钥是否以安全方式存储、更新密钥。

9.2.5 密钥销毁（FCS_CKM.4）

测评目的：

验证网银系统USBKey对交易签名算法相关密钥的销毁方法。

测评内容：

网银系统USBKey是否使用新密钥覆盖的方法来销毁交易签名算法相关密钥。

测评方法：

a) 通过指令多次生成交易签名算法相关密钥；
b) 确认网银系统 USBKey 只存储最新生成的交易签名算法相关密钥，以往生成的交易签名算法相关密钥已不能被访问到；
c) 若网银系统 USBKey 开发者使用其他密钥销毁方法，可按其方法内容进行验证。

9.2.6 密码运算（FCS_COP.1）

测评目的：

验证网银系统USBKey实现的密码算法功能。

测评内容：

网银系统USBKey是否正确实现DES，TDES，RSA，SHA-1（或符合国家密码主管部门要求的其他算法）及MAC操作等算法。

测评方法：

a) 通过指令执行 DES（64bits），TDES（128bits），RSA（2048bits），SHA-1 及 MAC（112bits）运算；
b) 利用密码工具执行同样的运算，并验证网银系统 USBKey 运算结果的正确性；
c) 若网银系统 USBKey 开发者使用其他密钥长度或其他算法，可按照其特定密钥长度及算法特性进行验证。

9.2.7 随机数生成（FCS_RNG.1）

测评目的：

验证网银系统USBKey实现的随机数生成功能。

测评内容：

网银系统USBKey是否正确实现随机数生成功能且生成的随机数满足相关标准要求的随机数质量要求。

测评方法：

a) 通过指令读取网银 USBKey 随机数发生器产生的随机数；
b) 对产生的随机数执行频数检测、累加和检测、线性复杂度检测、重叠子序列检测、Maurer 通用统计检测、矩阵秩检测、游程分布检测、扑克检测、块内频数检测、离散傅里叶检测、游程总数检测、块内最大 1 游程检测、自相关检测、近似熵检测、二元推导检测、重叠模板匹配检测、非重叠模板匹配检测等检测项；
c) 检查源代码，验证软件正确调用了芯片所提供的随机数安全生成算法。

9.2.8 子集访问控制（FDP_ACC.1）

测评目的：

验证网银系统USBKey实现的对交易签名和签名公私钥的访问控制功能。

测评内容：

a) 网银系统 USBKey 用户对交易数据的签名控制；

b) 网银系统 USBKey 用户对签名公私钥的访问控制。

测评方法：

具体内容见9.2.9条的测评方法。

9.2.9 基于安全属性的访问控制（FDP_ACF.1）

测评目的：

验证网银系统USBKey实现的对交易签名和签名公私钥的访问控制功能。

测评内容：

a) 网银系统 USBKey 用户对交易数据的签名控制；

b) 网银系统 USBKey 用户对签名公私钥生成的控制。

测评方法：

a) 在通过 PIN 验证及按键确认的验证方式下，验证对交易数据的签名控制；

b) 在通过 PIN 验证及按键确认的验证方式下，验证对公私钥生成的控制；

c) 若网银系统 USBKey 开发者使用其他验证方式，需在其他验证方式下验证对交易数据的签名控制及对公私钥生成的控制；

d) 验证在执行这些操作时，网银系统 USBKey 是否以明确的方式提示用户，如声音、指示灯、屏显等方式。

9.2.10 子集残余信息保护（FDP_RIP.1）

测评目的：

验证网银系统USBKey对交易签名密钥对和PIN码残余信息的处理功能。

测评内容：

网银系统USBKey是否正确实现对交易签名密钥对和PIN残余信息的处理功能：

a) 新的交易签名密钥对生成后，相关的旧密钥对失效，无法继续使用；

b) 网银系统 USBKey 使用完交易签名密钥对和 PIN 后，应及时清除 RAM 中的信息；

c) 用户输入及使用完 PIN 后，中间件应及时清除 PIN。

测评方法：

a) 查看源代码，确认交易签名密钥对生成后，USBKey 会对旧密钥对的有效性进行正确处理，使其无法继续使用；向 USBKey 发送相应指令，确认旧密钥对已无法使用；

b) 查看源代码，确认 USBKey 在使用完交易签名密钥对和 PIN 后，会及时删除 RAM 中的相应信息；

c) 查看源代码，确认 USBKey 中间件在使用完 PIN 后，会及时清除 PIN；并通过内存扫描工具确认 PIN 确已清除。

9.2.11 基本回退（FDP_ROL.1）

测评目的：

验证网银系统USBKey在相关安全操作发生时用于签名的PIN安全状态的回退功能。

测评内容：

网银系统USBKey是否正确实现在签名数据格式错误、签名流程被破坏、签名成功、签名取消操作、签名超时的条件等发生时，用于签名的PIN安全状态及相关数据内容进行回退。

测评方法：

a) 执行签名数据格式错误、签名流程被破坏、签名成功、签名取消操作、签名超时等相关操作；
b) 查看用户签名的 PIN 的安全状态，确认其是否已回退到未成功鉴别状态；
c) 若网银系统 USBKey 开发者使用其他操作，需在其他操作下验证用户签名的 PIN 的安全状态及相关数据内容是否发生回退。

9.2.12 鉴别失败处理（FIA_AFL.1）

测评目的：

验证网银系统USBKey对PIN鉴别失败后的处理功能。

测评内容：

网银系统USBKey是否正确实现对PIN鉴别相关剩余尝试次数的记录,以及验证失败达到一定次数后采取提示或锁定PIN的操作。

测评方法：

a) 执行多次错误的 PIN 验证和修改操作，确认 PIN 鉴别失败时 USBKey 是否进入安全状态；
b) 当 PIN 连续鉴别错误达到一定次数时，确认网银系统 USBKey 是否提示用户确认该鉴别操作；
c) 当 PIN 连续鉴别错误数达到赋值次数时，确认网银系统 USBKey 是否锁定 PIN。

9.2.13 鉴别的时机（FIA_UAU.1）

测评目的：

验证网银系统USBKey允许用户在其身份被鉴别前执行某些动作的功能。

测评内容：

网银系统USBKey是否正确实现在用户身份被鉴别之前可执行除交易数据签名、密钥对生成之外的操作。

测评方法：

a) 不进行 PIN 验证，执行交易数据签名、密钥对生成操作，确认操作不能成功执行；
b) 不进行 PIN 验证，执行其他操作，如读取 USBKey 基本信息，确认操作可成功执行；
c) 若网银系统 USBKey 开发者使用其他金融安全操作，需确认在不进行 PIN 验证时这些操作不能成功执行。

9.2.14 一次性鉴别机制（FIA_UAU.4）

测评目的：

验证网银系统USBKey对PIN鉴别数据的防重放功能。

测评内容：

网银系统USBKey是否正确实现防止与PIN验证鉴别机制有关的鉴别数据的再次使用。

测评方法：

a) 执行成功的 PIN 鉴别并抓取相应数据包；
b) 对该数据包进行回放，确认回放的数据包不能通过 PIN 验证。

9.2.15 多重鉴别机制（FIA_UAU.5）

测评目的：

验证网银系统USBKey支持多种鉴别机制对交易签名用户身份进行鉴别。

测评内容：

网银系统USBKey是否正确实现通过PIN验证和按键确认的用户鉴别机制来鉴别交易签名用户所声称的身份。

测评方法：

a) 确认交易签名用户需 PIN 验证通过且按键确认来鉴别身份，鉴别通过后可执行交易签名；
b) 若网银系统 USBKey 开发者使用其他鉴别机制及其规则，需验证是否在该鉴别机制及规则下对交易签名用户身份进行鉴别。

9.2.16 标识的时机（FIA_UID.1）

测评目的：

验证网银系统USBKey允许用户在被识别前执行某些动作。

测评内容：

网银系统USBKey是否正确实现用户在被识别前可执行除交易数据签名、密钥对生成之外的操作。

测评方法：

具体内容见9.2.13条的测评方法。

9.2.17 安全功能行为的管理（FMT_MOF.1）

测评目的：

验证网银系统USBKey允许授权用户管理指定安全属性的功能。

测评内容：

网银系统USBKey是否正确实现仅限管理员角色能够解锁PIN和初始化USBKey。

测评方法：

a) 执行成功的管理员 PIN 验证后进行解锁 PIN 和初始化 USBKey 操作，确认可成功执行；
b) 确认其他角色不能成功执行解锁 PIN 和初始化 USBKey 操作。

9.2.18 安全功能数据的管理（FMT_MTD.1）

测评目的：

验证网银系统USBKey允许授权用户管理安全功能数据的功能。

测评内容：

网银系统USBKey是否正确实现仅限管理员角色能够对PIN值、PIN验证失败次数和USBKey中存储的相关维护密钥进行管理。

测评方法：

a) 执行成功的管理员 PIN 验证后对 PIN 值、PIN 验证失败次数进行重置操作，对 USBKey 中存储的相关维护密钥进行修改操作；
b) 验证 PIN 码修改应需要验证用户权限，即应通过 PIN 验证通过；
c) 分析文档、代码等相关资料，检查安全数据是否以安全的方式存储。

9.2.19 管理功能规范（FMT_SMF.1）

测评目的：

验证网银系统USBKey对生命周期的管理功能。

测评内容：

网银系统USBKey是否正确实现对UABKey生命周期应用初始和使用配置阶段相关指令、操作的控制和管理。

测评方法：

a) 执行应用初始和使用配置各阶段相关指令和操作，确认可成功执行；
b) 执行非本生命周期阶段内的相关指令和操作，确认其不能成功执行。

9.2.20 安全角色（FMT_SMR.1）

测评目的：

验证网银系统USBKey与安全相关的角色。

测评内容：

网银系统USBKey是否正确实现授权用户和管理员的角色划分并将用户与角色进行关联。

测评方法：

a) 验证进行 PIN 验证后可成为授权用户角色；
b) 验证管理员 PIN 后可成为管理员角色。

9.2.21 物理攻击抵抗（FPT_PHP.3）

测评目的：

验证网银系统USBKey物理攻击抵抗的功能。

测评内容：

网银系统USBKey是否能抵抗逆向分析、侧信道攻击、差错注入攻击、侵入式攻击。

测评方法：

a) 对中间件实施逆向分析，确认中间件是否采用了相关安全措施；
b) 对 USBKey 实施侧信道攻击，如功耗分析、电磁分析等，确认其是否采用了相关安全措施；
c) 对 USBKey 实施差错注入攻击，如如光攻击、电压毛刺注入、电磁操纵等错误注入方法，确认其是否采用了相关安全措施；
d) 对 USBKey 实施侵入式分析，如芯片剖片、电路重构、电路探测和修改等，确认其是否采用了相关安全措施；
e) 对 USBKey 实施环境压力测试，如异常环境温度、异常工作电压、异常工作频率、静电等方法，确认其是否采用了相关安全措施；
f) 针对芯片的更详细的物理安全测试方法参见 JR/T 0098.2，至少包括该标准中所有的测试项。

9.2.22 功能恢复（FPT_RCV.4）

测评目的：

验证网银系统USBKey失效发生后安全功能应恢复到安全状态的功能。

测评内容：

网银系统USBKey是否正确实现掉电和按键持续导通发生时，相关安全功能恢复到一个安全状态。

测评方法：

a) 在执行生成密钥对、PIN 验证、PIN 修改操作过程中，网银系统 USBKey 发生掉电，确认操作或者成功完成，或者出现指明的失败情况后，应恢复到一个安全状态；
b) 按键持续导通发生时，确认与按键确认相关的操作不能成功完成，应恢复到一个安全状态。

9.2.23 重放检测（FPT_RPL.1）

测评目的：

验证网银系统USBKey对相关数据重放的检测功能。

测评内容：

网银系统USBKey是否正确实现对PIN验证数据、PIN修改数据、USBKey屏显的签名交易数据的重放，并在检测到重放后执行相应的处理操作。

测评方法：

a) 执行成功的 PIN 验证、PIN 修改及下发 USBKey 屏显的签名交易数据，并抓取相应数据包；
b) 对该数据包进行回放，确认网银系统 USBKey 对回放的数据包拒绝操作并复位安全状态；
c) 若网银系统 USBKey 开发者使用其他安全操作，需验证网银系统 USBKey 检测到重放时是否执行该安全操作。

9.2.24 内部 TSF 数据传送的基本保护（FPT_ITT.1）

测评目的：

验证网银系统USBKey对其不同部分间传送的安全功能数据的保护功能。

测评内容：

网银系统USBKey是否正确实现PIN、密钥等安全功能数据在内部传输时不被泄露和修改。

测评方法：

a) 通过分析中间件到 USBKey 间传送的相关数据包，确认数据在传送过程中被进行了保护，并以安全的方式在链路上进行传输；
b) 分析文档和源代码确认不存在安全数据被输出的情况，如从 USBKey 内部输出 PIN。

9.2.25 原发会话终止（FTA_SSL.3）

测评目的：

验证网银系统USBKey在用户在一段时间不活动后终止该会话的功能。

测评内容：

网银系统USBKey是否正确实现在超过约定的时间间隔后终止该交互式会话。

测评方法：

a) 一段时间无任何操作，或执行需要用户按键确认的操作并不执行按键动作直到超出约定时间；
b) 确认网银系统 USBKey 是否终止该交互式会话，是否通过语音或屏幕显示提醒告知用户。

9.3 安全保证要求测评要求

9.3.1 授权控制（ACM_CAP.3）

测评目的：

a) 确保网银系统 USBKey 在发送给用户之前是正确的和完备的；
b) 确保在评估过程中没有遗漏配置项；
c) 防止对网银系统 USBKey 配置项进行未授权地修改、增加或删除。

测评内容：

a) 确认开发者提供的网银系统 USBKey 参照号对 TOE 的每一个版本是唯一的；
b) 确认网银系统 USBKey 被标记上参照号；
c) 确认 CM 文档应包括一个配置清单和一个 CM 计划；
d) 确认配置清单唯一标识组成网银系统 USBKey 的所有配置项；
e) 确认配置清单描述组成网银系统 USBKey 的配置项；
f) 确认 CM 文档应描述用于唯一标识网银系统 USBKey 所包含配置项的方法；
g) 确认 CM 系统应唯一标识网银系统 USBKey 所包含的所有配置项；
h) 确认 CM 计划应描述 CM 系统是如何使用的；

i) 确认 CM 系统的运行与 CM 计划是一致的；
j) 确认 CM 文档提供所有配置项都已经和正在 CM 系统下有效地进行维护的证据；
k) 确认 CM 系统提供措施使得只能对配置项进行授权改变。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；
b) 部分测评内容通过现场核查确认。审计配置管理中的 USBKey 源代码是否与设计要求一致。

9.3.2 TOE CM 覆盖（ACM_SCP.1）

测评目的：

确保所要求的所有评估证据都置于CM之下，并可以确保它们的修改是在正确授权的受控方式下进行的。

测评内容：

确保开发者提供的网银系统USBKey配置项列表包括实现表示和ST中其他保证组件所要求的评估证据。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.3 交付程序（ADO_DEL.1）

测评目的：

确保网银系统USBKey在分发过程中的安全性。

测评内容：

a) 确保开发者提供的交付文档描述了在向用户方分发 TOE 版本时，用以维护其安全性所必需的所有程序；
b) 确认开发者提供的交付文档中描述的交付程序正在被使用。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；
b) 部分测评内容通过现场核查确认。

9.3.4 安装、生成和启动程序（ADO_IGS.1）

测评目的：

确保网银系统USBKey以开发者所期望的安全方式进行安装、生成和启动。

测评内容：

a) 确保开发者提供的安装、生成和启动程序文档描述 TOE 安全地安装、生成和启动必需的所有步骤；
b) 确保安装、生成和启动程序文档描述的安装、生成和启动程序最终产生了一个安全的配置。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.5 非形式化功能规范（ADV_FSP.1）

测评目的：

确保开发者提供的功能规范是用户可见接口和安全功能行为的一个高层描述。

测评内容：

a) 确保开发者提供的功能规范应使用非形式化风格来描述 TSF 及其外部接口；

b) 确保开发者提供的功能规范是内在一致的；
c) 确保开发者提供的功能规范描述所有外部安全功能接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
d) 确保开发者提供的功能规范完备地表示安全功能，是网银系统 USBKey 安全功能要求的一个准确且完备的实例化。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.6 安全加强的高层设计（ADV_HLD.2）

测评目的：

确保开发者提供的高层设计按照主要的结构单元(即子系统)描述网银系统USBKey的安全功能，并将这些单元同所提供的功能相联系。

测评内容：

a) 确保开发者提供的高层设计的是非形式化的；
b) 确保开发者提供的高层设计是内在一致的；
c) 确保开发者提供的高层设计按子系统描述网银系统 USBKey 的安全功能的结构；
d) 确保开发者提供的高层设计描述每个网银系统 USBKey 的安全功能子系统所提供的安全功能性；
e) 确保开发者提供的高层设计标识网银系统 USBKey 的安全功能所要求的任何基础性硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 确保开发者提供的高层设计标识网银系统 USBKey 的安全功能子系统的所有接口；
g) 确保开发者提供的高层设计标识网银系统 USBKey 的安全功能子系统的哪些接口是外部可见的；
h) 确保开发者提供的高层设计描述网银系统 USBKey 的安全功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
i) 确保开发者提供的高层设计把 TOE 分成 TSP-实施和其他子系统来描述。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.7 非形式化对应性证实（ADV_RCR.1）

测评目的：

确保开发者提供的概要规范、功能规范、高层设计之间的对应性分析是准确的、一致的。

测评内容：

开发者提供的网银系统USBKey的安全功能表示的所有相邻对之间对应性的分析证实，较为抽象的网银系统USBKey的安全功能表示的所有相关安全功能都在较不抽象的网银系统USBKey的安全功能表示中得到正确且完备地细化。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.8 管理员指南（AGD_ADM.1）

测评目的：

确保开发者提供的管理员指南为网银系统USBKey的管理员描述了如何正确管理并最大限度地保证网银USBKe安全，帮助管理员理解TOE提供的安全功能。

测评内容：

a) 开发者提供的管理员指南描述网银系统 USBKey 管理员可使用的管理功能和接口；
b) 开发者提供的管理员指南应描述如何以安全的方式管理网银系统 USBKey；
c) 开发者提供的管理员指南包含一些关于安全处理环境中应被控制的功能和特权的警示信息；
d) 开发者提供的管理员指南描述所有关于与 TOE 安全运行有关用户行为的假设；
e) 开发者提供的管理员指南描述所有受管理员控制的安全参数，适当时应指明安全值；
f) 开发者提供的管理员指南描述每一种与需要执行的管理功能有关的安全相关事件，包括改变网银系统 USBKey 的安全功能所控制实体的安全特性；
g) 开发者提供的管理员指南与供评估的所有其他文档保持一致；
h) 开发者提供的管理员指南描述所有与管理员有关的 IT 环境安全要求。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.9 用户指南（AGD_USR.1）

测评目的：

确保开发者提供的用户指南描述了网银系统USBKey提供的安全功能，以及提供网银系统USBKey安全使用的一些规程和指导。

测评内容：

a) 开发者提供的用户指南描述网银系统 USBKey 的非管理员用户可使用的功能和接口；
b) 开发者提供的用户指南描述网银系统 USBKey 所提供的用户可访问安全功能的使用；
c) 开发者提供的用户指南包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；
d) 开发者提供的用户指南应清晰地阐述网银系统 USBKey 安全运行所必需的所有用户职责，包括与网银系统 USBKey 安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；
e) 开发者提供的用户指南应与供评估的所有其他文档保持一致；
f) 开发者提供的用户指南应描述所有与用户有关的 IT 环境安全要求。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.10 安全措施标识（ALC_DVS.1）

测评目的：

确保网银系统USBKey的开发环境采取了物理的、程序的、人员的以及其他的为保护网银系统USBKey而在开发环境中采用的安全措施，包括开发场地的物理安全和任何用于选择开发人员的程序。

测评内容：

a) 开发者提供的开发安全文档描述在网银系统 USBKey 的开发环境中，保护网银系统 USBKey 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施；
b) 开发安全文档提供在网银系统 USBKey 的开发和维护过程中执行安全措施的证据。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；
b) 部分测评内容通过现场核查确认。

9.3.11 覆盖分析（ATE_COV.2）

测评目的：

确保开发者已经按照功能规范对网银系统USBKey安全功能进行了测试。

测评内容：

a) 开发者提供的测试覆盖分析证实测试文档中所标识的测试与功能规范中所描述的网银系统USBKey 安全功能之间的对应性；

b) 开发者提供的测试覆盖分析证实功能规范中所描述网银系统 USBKey 安全功能与测试文档所标识的测试之间的对应性是完备的。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.12 测试：高层设计（ATE_DPT.1）

测评目的：

确保开发者已经按照高层设计对网银系统USBKey在子系统级别上进行了测试。

测评内容：

开发者提供的深度分析证实测试文档中所标识的测试足以证实该网银系统USBKey安全功能是依照其高层设计运行的。

测评方法：

评估者应确认开发者所提供的证据满足测评内容的所有要求。

9.3.13 功能测试（ATE_FUN.1）

测评目的：

确保开发者执行了测试并提供的测试文档证实所有的安全功能都按照规定执行。

测评内容：

a) 开发者提供的测试文档包括测试计划、测试程序描述、预期的测试结果和实际的测试结果；

b) 开发者提供的测试文档标识要测试的安全功能和描述要执行的测试的目标；

c) 开发者提供的测试文档标识要执行的测试和描述每个安全功能的测试脚本，这些脚本包括对于其他测试结果的任何顺序依赖性；

d) 开发者提供的测试文档中预期的测试结果指出测试成功执行后的预期输出；

e) 开发者执行测试所得到的测试结果证实每个被测试的安全性功能都按照规定运转。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；

b) 部分测评内容通过独立测试—抽样（ATE_IND.2）确认。

9.3.14 独立测试—抽样（ATE_IND.2）

测评目的：

证实安全功能按照规定执行。

测评内容：

a) 评估者执行测试文档中的一个测试样本，以验证开发者的测试结果；

b) 评估者应测试 TOE 所有安全功能，以确认 TOE 按照规定运行。

测评方法：

评估者对开发者测试文档中的测试样本进行抽样测试，并对TOE所有安全功能进行测试。

9.3.15 指南审查(AVA_MSU.1)

测评目的：

确保指导性文档中不会存在容易误解的、不切实际的和前后矛盾的指南，而且所有运行模式的安全程序都得到了处理，不安全的状态应是易于检测的。

测评内容：

a) 开发者提供的指导性文档标识所有可能的 TOE 运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义；
b) 开发者提供的指导性文档是完备的、清晰的、一致的、合理的；
c) 开发者提供的指导性文档列出关于预期使用环境的所有假设；
d) 开发者提供的指导性文档列出对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；
b) 部分测评内容结合安装、生成和启动程序（ADO_IGS.1）和用户指南（AGD_USR.1）确认。

9.3.16 TOE 安全功能强度评估(AVA_SOF.1)

测评目的：

确认开发者对相关安全机制的安全功能强度分析是合理的。

测评内容：

a) 开发者对 ST 中所标识的每个具有 TOE 安全功能强度声明的安全机制进行 TOE 安全功能强度分析；
b) 对于每个具有 TOE 安全功能强度声明的安全机制，TOE 安全功能强度分析说明该机制达到或超过 PP/ST 中定义的最低强度级别；
c) 对于每个具有特定 TOE 安全功能强度声明的安全机制，TOE 安全功能强度分析应说明该机制达到或超过 PP/ST 中定义的特定功能强度度量。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；
b) 部分测评内容结合非形式化功能规范（ADV_FSP.1）、安全加强的高层设计（ADV_HLD.2）确认开发者强度声明是正确的。

9.3.17 高级抵抗力（AVA_VLA.4）

测评目的：

确保网银系统USBKey能抵抗具有高等攻击潜力的攻击者发起的攻击。

测评内容：

a) 开发者提供的脆弱性分析文档描述为搜索用户能违反 TSP 的方法而执行的 TOE 可交付材料分析；
b) 开发者提供的脆弱性分析文档描述对已标识的脆弱性的处置；
c) 开发者提供的脆弱性分析文档针对所有已标识的脆弱性，说明脆弱性不能在 TOE 的预期使用环境中被利用；
d) 开发者提供的脆弱性分析文档应证明存在已标识脆弱性的 TOE 可以抵御明显的穿透性攻击。

测评方法：

a) 评估者应确认开发者所提供的证据满足测评内容的所有要求；
b) 评估者应在开发者脆弱性分析的基础上实施穿透性测试，以确保已标识的脆弱性都已被处理；

c) 评估者应基于独立的脆弱性分析，执行独立的穿透性测试，以决定在预期使用环境中额外的已标识脆弱性不可被利用；评估者应对 6.4 条中列出的所有威胁进行分析，以确认用以抵抗这些威胁的设计可满足安全要求；

d) 评估者应在开发者脆弱性分析的基础上实施包括但不限于：功耗分析、电磁分析、激光操纵攻击、侵入式等攻击测试。针对芯片的更详细的测试方法可参见 JR/T 0098.2；

e) 评估者应决定 TOE 可以抵御拥有高等攻击潜力的攻击者发起的穿透性攻击。