

密码检测报告

报告编号：CCTC-SF36-2022-0309



产品名称： 应用安全软件密码模块（Linux 版）

型号规格： AS-TSCM

版本号： 8.3.1

委托方： 蚂蚁科技集团股份有限公司

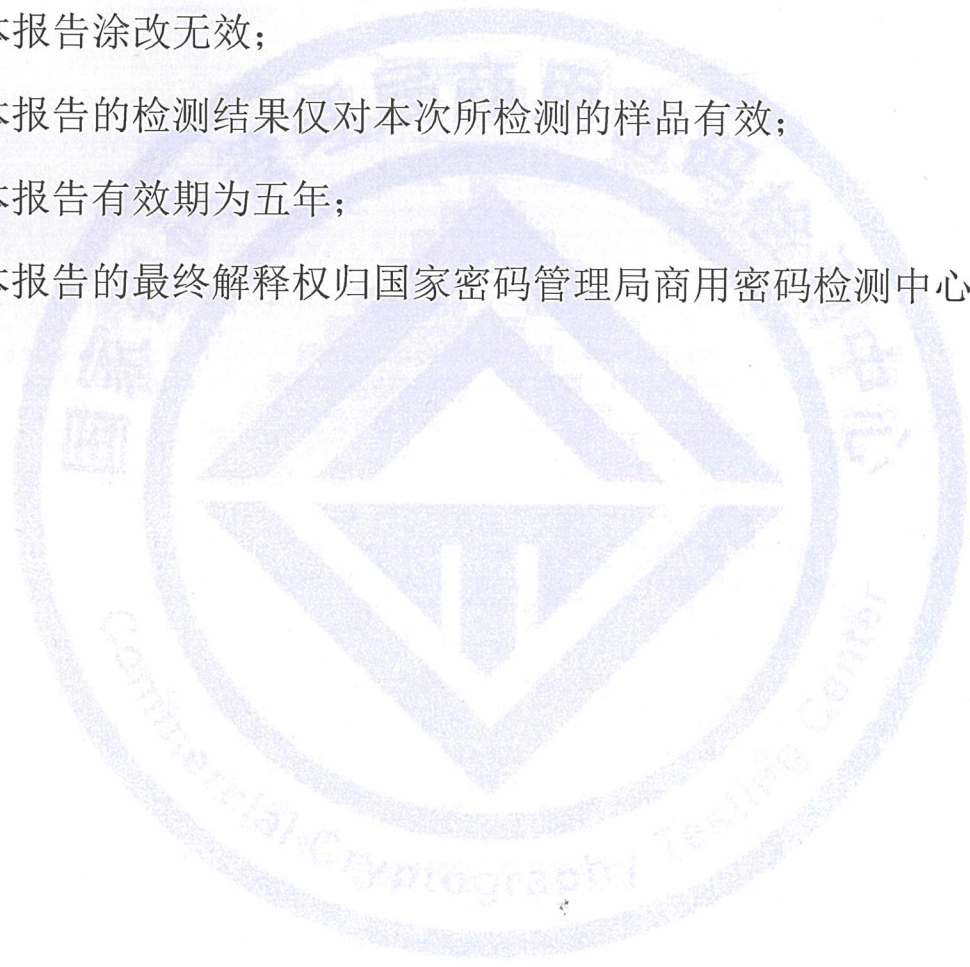
国家密码管理局商用密码检测中心

2022年11月18日



声明

- 1.本报告无检测机构公章无效；
- 2.本报告未经检测机构允许，不得部分复制；
- 3.复制本报告未重新加盖检测机构公章无效；
- 4.本报告涂改无效；
- 5.本报告的检测结果仅对本次所检测的样品有效；
- 6.本报告有效期为五年；
- 7.本报告的最终解释权归国家密码管理局商用密码检测中心所有。



1871
2022



1 基本信息

委托方	名称	蚂蚁科技集团股份有限公司
	通信地址	杭州市西湖区西溪新座 5 幢 802 室
	统一社会信用代码	913301067046373179
	电话	0571-26888888
	传真	0571-86432799
	手机	15010370275
	联系人	张成龙
检测机构	名称	国家密码管理局商用密码检测中心
	通信地址	北京市丰台区万丰路 300 号 1 号楼一层
	电话	010-83298576
	传真	010-83298578
样品信息	产品名称	应用安全软件密码模块 (Linux 版)
	型号规格	AS-TSCM
	版本号	8.3.1
	出厂编号 /SN 码	/
检测日期	2022 年 8 月 3 日 至 2022 年 11 月 18 日	

2 检测依据及参考标准

GM/T 0028 《密码模块安全技术要求》

GM/T 0039 《密码模块安全检测要求》



3 产品情况

送检产品是一款为操作系统上的应用程序提供单向 TLCP 通信协议的软件密码模块。送检产品为运行在 Linux 操作系统上的可执行文件，由初始化、基础密码学原语、传输层安全通信模块组成。送检产品由 C 语言软实现 SM2、SM3、SM4 密码算法，其中，SM2 算法主要用于身份认证及软件完整性校验，SM3 算法用于数据完整性验证，SM4 算法用于数据加解密。随机数由密码模块使用运行环境采集器采集的可变信息（系统内核的随机数发生器、系统中断事件、系统时间），通过基于 SM3 算法的 DRNG 处理后产生。送检产品采用单向 TLCP 协议 ECC (SM2) _SM4_SM3 算法套件实现数据传输。

部署环境照片	<pre>[root@centos7 ~]# lscpu Architecture: x86_64 CPU op_mode(s): 32-bit, 64-bit Byte Order: Little Endian CPU(s): 4 On-line CPU(s) list: 0-3 Thread(s) per core: 1 Core(s) per socket: 4 Socket(s): 1 NUMA node(s): 1 Vendor ID: GenuineIntel CPU family: 6 Model: 142 Model name: Intel(R) Core(TM) i7-7660U CPU @ 2.50GHz Stepping: 9 CPU MHz: 2495.998 bogomips: 4991.99 Hypervisor vendor: kvm Virtualization type: full L1d cache: 32K L1i cache: 32K L2 cache: 256K L3 cache: 4096K NUMA node0 CPU(s): 0-3 Flags: tpu vme de pse tsc msr pae mce cx8 apic sep mtr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx xsave avx rdtscp lm hypervisorlahf_lm abm 3dnowprefetch invpcid_single fsgsbase avx2 invpcid rdseed clflushopt [root@centos7 ~]# free -g total used free shared buff/cache available Mem: 9 1 6 0 1 8 Swap: 3 0 3 0 0 0 [root@centos7 ~]# uname -a Linux centos7.linuximages.local 3.10.0-1160.6.1.el7.x86_64 #1 SMP Tue Nov 17 13:59:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux [root@centos7 ~]#</pre> <p>Intel (R) Core (TM) i7-7660U 处理器，Linux Centos 7 操作系统</p>
系统界面照片	<pre>BabaSSL> version -g BabaSSL 8.3.1 产品名称：应用安全软件密码模块（Linux版） 型号：AS-TSCM 公司：蚂蚁科技集团股份有限公司 BabaSSL></pre>



4 检测结果

检测项目		检测结果
功能检测	密码算法正确性检测	通过
	随机数质量检测	通过
	安装/初始化	符合
	版本查询	符合
	访问控制	符合
	密钥管理	符合
	置零功能	符合
	自测试	符合
	TLCP 安全通道	符合
	随机数熵源测试	符合
性能检测	每秒新建连接数	679.72 条/秒
	最大并发连接数	40000 条
	最大并发用户数	40000 条
	吞吐量	44.43Mbps
申报安全等级		安全等级第一级
密码模块安全等级检测	密码模块规格	通过
	密码模块接口	通过
	角色、服务和鉴别	通过
	软件/固件安全	通过
	运行环境	通过
	物理安全	不适用
	非入侵式安全	不适用
	敏感安全参数管理	通过



检测项目		检测结果
密码模块安全等级检测	自测试	通过
	生命周期保障	通过
	对其他攻击的缓解	不适用
	符合安全等级第一级	
检测的密码算法	SM2、SM3、SM4	
其他说明	性能指标为被测样品在检测环境下的测试结果	

经检测，蚂蚁科技集团股份有限公司送检的 AS-TSCM 型应用安全软件密码模块（Linux 版）符合 GM/T 0028《密码模块安全技术要求》安全等级第一级相关要求，通过密码检测。

国家密码管理局商用密码检测中心

2022年11月18日

