公安交通管理信息系统外挂软件安全管理规定

第一章　总则

第一条 为加强公安交通管理信息系统外挂软件安全管理，提高外挂软件安全设计水平，规范外挂软件管理工作流程，根据《公安交通管理信息系统运行管理规定》以及国家和公安部相关规定，制定本规定。

第二条 本规定所称外挂软件是指各级公安机关交通管理部门或者相关单位建设应用的，能够查询、写入、修改、删除公安交通管理综合应用平台、公安交通集成指挥平台以及机动车检验监管系统、机动车驾驶人考试监管系统等全国统一版信息系统数据的信息系统。

第三条 本规定适用于外挂软件的安全设计、安全测试、接口申请、访问授权、上线运行、下线停用等安全管理工作。

第四条 各级公安机关交通管理部门应当参照《公安交通管理综合应用平台安全保护通用技术要求》（GA/T 1168-2014）、国家和公安部关于信息安全的相关要求，建设外挂软件的安全运行环境，建立健全外挂软件运行和使用管理制度，加强日常安全监

管。

第五条 各级公安机关交通管理部门基于公安交通管理统一版核心信息系统应用库、分发库开发的应用软件，应参考本规定加强软件安全设计、安全测试和日常安全管理工作。

第二章　工作职责

第六条 外挂软件安全实行分级管理，各级公安机关交通管理部门以及公安部交通管理科学研究所应当按照工作职责，落实各项任务，加强安全管理。

第七条 公安部交通管理局负责以下事项:

（一）组织研究、制定外挂软件安全管理相关规章、制度、技术标准和规范，并组织实施;

（二）组织开发、推广、升级公安交通管理信息系统请求服务接口申请、授权、使用监管相关信息系统;

（三）审核外挂软件技术方案，组织测试，审批外挂软件接入申请;

（四）指导、监督、检查各地外挂软件建设应用和安全管理，组织对各地外挂软件请求服务接口使用情况进行监管、通报和安全事件处置。

第八条 省（区、市）及以下公安机关交通管理部门负责以下事项:

（一）落实公安部外挂软件安全相关规章、制度、技术标准和规范，制定本地外挂软件安全管理配套制度；

（二）组织本地外挂软件安全设计、研发、测试、接入申请等工作，对下级公安机关交通管理部门外挂软件安全设计、接口申请进行审核把关、汇总上报；

（三）组织本地外挂软件安全方案专家评审，对安全方案的完整性、合规性、科学有效性进行论证；

（四）建设外挂软件的安全运行环境，开展外挂软件访问监控、日志分析等日常安全管理工作；

（五）指导、监督、检查本地外挂软件及下级公安机关交通管理部门外挂软件建设应用和安全管理，组织对管辖范围内外挂软件请求服务接口使用情况进行监管、通报和安全事件处置。

第九条 公安部交通管理科学研究所负责以下事项：

（一）承担外挂软件安全管理相关规章、制度、技术标准和规范制定工作；

（二）承担公安交通管理信息系统请求服务接口申请、授权、使用监管相关信息系统的开发、升级、培训和推广应用工作；

（三）研究外挂软件请求服务接口安全管理技术，提高请求服务接口安全防护、监管、审计技术水平；

（四）承担外挂软件技术方案审核、安全测试、接入备案工作，在外挂软件接口申请通过公安部交通管理局审核后开展授权工作；

（五）协助公安部交通管理局指导、监督、检查各地外挂软件建设应用和安全管理，对各地外挂软件请求服务接口使用情况进行监管、通报和安全事件处置；

（六）定期抽检各地外挂软件运行环境、应用软件功能、日常安全管理是否符合本规定及相关信息安全管理规定要求。

第十条 各级公安交通管理部门应当按照《公安交通管理信息系统运行管理规定》要求，设立专职的信息安全管理员，由安全管理员负责外挂软件的安全管理工作。

第三章　外挂软件安全设计

第十一条 各级公安机关交通管理部门的外挂软件建设项目必须同步考虑安全问题，在外挂软件设计定义阶段，开展风险分析、安全需求分析和安全方案制定工作。

第十二条 风险分析应当以应用软件安全运行、数据安全保护、异常违规业务防范为出发点，全面分析由于物理的、系统的、管理的以及人为等原因所造成的安全风险。

第十三条 安全需求分析应当包含以下基本内容：

（一）针对风险分析发现的每一项安全风险和隐患确认安全需求；

（二）分析并确认外挂软件的整体安全需求；

（三）分析并确认应用软件安全运行的环境条件需求；

（四）分析并确认应用软件所实现的安全功能需求;

（五）列出可能的不期望事件，分析导致这些不期望事件的可能原因，提出相应的软件处理要求。

第十四条 制定安全方案时，应当针对安全需求分析中确认的每一项安全需求制定相应的安全策略和安全机制，并对其进行详细描述。

第十五条 外挂软件应当通过全国统一版信息系统提供的请求服务接口查询、写入、修改、删除全国统一版信息系统的数据，不允许以数据库授权访问、数据库链路等方式直接访问全国统一版信息系统数据库。

第十六条 全国统一版信息系统提供的请求服务接口不能满足需要的，应当将相关数据访问需求报公安部交通管理局，经公安部交通管理局研究确认具有全国共性需求的，组织完善请求服务接口功能。

各地可以基于本地应用库、分发库设计实现个性化请求服务功能，但应符合本规定的安全设计要求，数据抽取应遵循按需最小化抽取原则，不抽取手机号码、联系住所地址、车辆轨迹等个人隐私信息。

第十七条 外挂软件应用安全设计应当满足本规定附件《公安交通管理信息系统外挂软件安全设计规范》的基本要求，在身份鉴别、访问控制、安全审计、数据保护、软件容错、资源控制等方面进行安全设计。

第十八条 外挂软件不得以任何理由留有后门程序或者绕过软件的安全机制。

第十九条 申请单位应当组织外挂软件安全方案专家评审，对安全方案的完整性、合规性、科学有效性进行论证并通过专家评审。

第四章　外挂软件安全测试

第二十条 外挂软件正式上线运行前应当按照《公安交通管理信息系统运行管理规定》第七条和第二十一条、《公安交通管理综合应用平台使用规定》第四十六条、《互联网交通安全综合服务管理平台运行和使用规定（试行）》第十二条和第四十一条等管理规定，通过软件安全测试，未通过安全测试的外挂软件不允许上线运行。

第二十一条 外挂软件安全测试应当提交但不仅限于以下资料:

（一）外挂软件安全需求分析报告，其内容应当符合本规定第十三条要求;

（二）外挂软件技术方案，其内容应当包含信息安全技术方案并符合本规定第十四条要求;

（三）外挂软件操作说明;

（四）外挂软件请求服务接口调用情况说明，应当具体说明

每一个功能菜单、调用场景所需请求的服务接口，并与外挂软件操作说明内容实现对应。

第二十二条 外挂软件安全测试机构在完成测试后，出具安全测试报告，安全测试报告应当注明所测软件的版本编号。

第二十三条 安全测试应当至少包含以下内容:

（一）根据本规定第十五条、第十七条、第十八条及附件《公安交通管理信息系统外挂软件安全设计规范》的要求，对外挂软件安全设计、访问全国统一版信息系统方式等进行测试;

（二）核实外挂软件功能是否存在违规业务办理功能，是否符合相关法律法规的规定;

（三）对外挂软件请求服务接口调用需求进行确认;

（四）采用应用软件漏洞扫描软件对外挂软件进行安全扫描，测试外挂软件是否存在“中危”及以上风险漏洞。

第二十四条 当外挂软件发生涉及软件安全设计、请求服务接口需求调整及其他重大功能调整的，应当通过安全测试。

第五章　外挂软件请求服务接口申请和授权

第二十五条 外挂软件请求服务接口申请包括开发测试接口申请、正式上线运行接口申请、已授权接口调整申请三类。

第二十六条 外挂软件开发测试阶段，可以申请全国统一版信息系统提供的请求服务接口用于开发测试工作，但应当符合以

下要求:

（一）外挂软件名称应当在结尾处标注“开发测试阶段”;

（二）每个接口的日访问量不得超过100次;

（三）外挂软件有效期最长不得超过半年;

（四）IP地址设置最多不超过3个;

（五）外挂软件开发测试工作应当符合公安部关于公安内外网边界交换等安全管理规定,且外挂软件与全国统一版信息系统请求服务接口进行联调测试应当在相关责任民警的监督下开展。

第二十七条 外挂软件开发测试接口申请、授权工作流程如下:

（一）通过全国统一版信息系统填报并上传接口申请信息、外挂软件技术方案;

（二）省（区、市）公安交通管理部门审核后，报公安部交通管理科学研究所;

（三）公安部交通管理科学研究所对接口申请进行审核，审核通过的生成接口授权码，并向公安部交通管理局报备;

（四）下载接口授权码，开通使用。

第二十八条 已通过安全测试的外挂软件，可以申请正式上线运行接口，其申请、授权工作流程如下:

（一）通过全国统一版信息系统填报并上传接口申请信息,以及外挂软件技术方案等相关资料,相关资料具体内容和要求见第二十九条;

（二）省（区、市）公安交通管理部门审核后，报公安部交通管理科学研究所;

（三）公安部交通管理科学研究所审核后，报公安部交通管理局;

（四）公安部交通管理局完成审核后，公安部交通管理科学研究所生成接口授权码;

（五）下载接口授权码，开通使用。

第二十九条 正式上线运行接口申请，应当提交以下资料:

（一）本规定第二十一条所要求的外挂软件安全测试提交的相关资料;

（二）外挂软件安全测试机构出具的安全测试报告;

（三）外挂软件在本次申请单位的实际网络部署架构、安全防护情况说明，涉及公安内外网数据交换的，应当详细说明数据交换方案;

（四）每个接口日访问量设置的测算依据说明;

（五）除本规定所要求的安全测试外，对于国家或者行业标准另有明确设计要求，或者国家和公安部相关规定要求必须通过的测试内容，还应当提供相应的测试报告。

第三十条 对于正式上线运行接口申请，应当重点审核以下内容:

（一）外挂软件是否已通过安全测试，软件版本是否一致，提交材料是否齐全;

（二）申请的接口与安全测试报告确认的接口调用需求是否一致;

（三）外挂软件网络部署、数据交换是否符合公安部相关安全管理规定，接口日访问量设置是否合理。

第三十一条 已授权访问的外挂软件，在需要调整接口日访问量、访问 IP 地址、延长有效期时，可提交接口调整申请。申请、授权工作流程如下:

（一）通过全国统一版信息系统填报并上传接口调整申请信息，如涉及增加访问量的，还应上报增加访问量测算依据;

（二）省（区、市）公安交通管理部门审核后，报公安部交通管理科学研究所;

（三）公安部交通管理科学研究所对接口申请进行审核，更新授权信息，并向公安部交通管理局报备;

（四）下载更新接口授权信息。

第三十二条 已授权访问的外挂软件，需要增加访问接口的，按照本规定第二十八条、二十九条、三十条正式上线运行接口申请的流程和要求办理。

第三十三条 不允许未经安全测试、接口申请、授权的外挂软件共用已授权外挂软件的授权认证信息。

第六章　外挂软件下线停用

第三十四条 外挂软件不再使用的，应当及时卸载应用软件，清理外挂软件服务器，并申请取消外挂软件接口访问授权，防止外挂软件接口访问授权被违规使用。

第三十五条 外挂软件取消接口访问授权应当按照以下流程办理:

（一）通过全国统一版信息系统填报并上传接口访问授权取消申请;

（二）公安部交通管理科学研究所取消外挂软件接口访问授权，并向公安部交通管理局报备;

（三）下载更新接口授权信息，外挂软件关闭停用。

第三十六条 不得保留下线停用外挂软件的接口访问授权信息，提供其他外挂软件调用或者用于其他目的。

第七章　监督管理

第三十七条 公安部交通管理局对各地外挂软件安全测试、请求服务接口申请、接口调用情况进行监督，定期通报。

第三十八条 公安部交通管理科学研究所应当完善外挂软件接口调用日志信息，并基于接口调用日志开展外挂软件异常访问分析预警工作，上报公安部交通管理局。

第三十九条 公安部交通管理科学研究所定期对各地已授权外挂软件进行抽检，并将抽检结果上报公安部交通管理局。

第四十条 对于抽检发现外挂软件运行环境不符合安全管理要求或者外挂软件存在安全漏洞的，应当责令使用单位限期整改，拒不整改的，由公安部交通管理科学研究所暂停该外挂软件接口授权。对于抽检发现安全测试时外挂软件与实际部署运行外挂软件不一致的，由公安部交通管理科学研究所暂停该外挂软件接口授权。

第四十一条 省（区、市）公安交通管理部门应当对本地外挂软件安全测试、请求服务接口申请、接口调用等情况进行监督，定期通报并上报公安部交通管理局。

第四十二条 各级公安交通管理部门应当建立外挂软件安全管理倒查机制，发现利用外挂请求服务接口窃取数据、违规办理业务以及提交虚假信息申请接口等行为的，依照相关规定追究相关单位和个人责任。

第四十三条 由于外挂软件运行环境或者外挂软件自身存在安全漏洞等原因，导致外挂软件被攻击，发生大量敏感信息泄露、遭受大规模网络攻击等重大安全事件时，相关公安机关交通管理部门应立即采取关停外挂软件等处置措施，并逐级上报公安部交通管理局。

第四十四条 外挂软件设计、研发、测试及运维等阶段中，有承建单位、运维单位、外包服务承担单位及相关人员参与的，应当对其进行资格审查，并签订安全保密协议。

第八章　附则

第四十五条 本规定与《公安交通管理综合应用平台使用规定》、《公安交通管理信息系统运行管理规定》不一致的，以本规定为准。

第四十六条 本规定自 2017 年 7 月 1 日起实施。

附件：公安交通管理信息系统外挂软件安全设计规范

附件：

公安交通管理信息系统外挂软件安全设计规范

1 范围

本规范旨在根据《公安交通管理信息系统外挂软件安全管理规定》的规定，对外挂软件应用程序安全设计提出必要的技术要求，为各级公安机关交通管理部门外挂软件安全设计、开发和安全测试提供依据。本规范不涉及外挂软件运行环境安全、日常安全管理等其他内容，相关内容请参考《公安交通管理信息系统外挂软件安全管理规定》及国家和公安部相关规定。

本规范内容中，带*号标注的为推荐性安全设计，不作为安全测试通过的强制依据。

2 参考文件

GB/T 22239 信息安全技术信息系统安全等级保护基本要求

GA/T 1168 公安交通管理综合应用平台安全保护通用技术条件要求

3 身份鉴别

用户身份鉴别包括对用户的身份进行标识和鉴别。应当从以下方面设计和实现外挂软件应用程序的用户身份鉴别。

3.1 用户注册

对外挂软件应用程序的注册用户，应当按以下要求设计和实现标识功能:

1、凡需进入外挂软件应用程序的用户，应当先进行注册登记。

2、外挂软件用程序的用户标识应当包含用户名、用户标识符（UID）、身份证明号码、警员编号或者员工编号、姓名等信息，对警员和非警员身份进行明确标识，并提供和启用用户身份唯一性检查功能，在外挂软件应用程序的整个生存周期实现用户标识符的唯一性，以及用户标识符、用户名、身份证明号码、警员编号或者员工编号、姓名之间的一致性。

3、*对提供单点登录的分布式应用软件系统，应当提供单点用户标识，且单点标识应当具有与常规标识相同的安全性。

4、*应当对用户标识信息进行统一管理，确保注册行为的合规性及标识信息的准确性，并确保其不被非授权地访问、修改或者删除。

3.2、用户登录

对登录到外挂软件应用程序的用户，应当按以下要求进行身份鉴别:

1、*具备公安数字证书用户身份鉴别功能，并可强制用户以公安数字证书鉴别机制进行用户身份鉴别。

2、*采用了公安数字证书或者生物特征鉴别机制的应用软件系统，对系统用户（如系统管理员、审计员和安全员）应当强制以公安数字证书或者生物特征鉴别机制进行身份鉴别。

3、应当提供用户密码校验功能，以确保用户密码长度不小于8位，且必须包含英文字符、数字及特殊符号。

4、鉴别信息应当是不可见的，并在传输时用加密方法或者具有相同安全强度的其他方法进行安全保护。

5、用户密码不允许在数据库中明文存储，应当以用户标识符、用户密码、姓名等鉴别信息组合后，用加密方法存储。

6、应当预先定义鉴别失败次数的阀值，当用户鉴别失败次数达到阀值时，外挂软件应用程序应当退出登录过程并终止与用户的交互，并将信息写入安全日志。

7、对重复鉴别行为的限制应当提供基于访问终端和基于用户两种方式，当某一访问终端鉴别失败次数达到阀值时，应当将该访问终端信息写入黑名单，在一定时间段内限制其再次登录;当某一用户鉴别失败次数达到阀值时，应当锁定该用户，限制其再次登录。对提供访问终端黑名单和用户解锁功能的，解锁操作

应当写入安全日志。

8、外挂软件应用程序应能通过设定用户有效期、密码有效期、IP/MAC 地址或者登录地点、登录时间段等手段对用户登录行为进行限制。

9、超过用户有效期的用户只有经系统管理员激活并延长有效期后方可登录外挂软件应用程序；该用户激活后，应当强制其修改密码，成功后方可登录，并延长密码有效期。

10、*对提供单点登录的分布式应用程序的用户应当提供单点用户鉴别，且单点鉴别应当具有与常规鉴别相同的安全性。

11、具备对同一用户多地、同时登录外挂软件应用程序的异常情况进行检测和限制的功能。

12、用户登录成功后，外挂软件应用程序应当记录并向用户显示日期、时间、来源和上次成功登录的日期、时间、来源，以及上次成功访问之后用户身份鉴别失败的情况、用户和密码距离到期的天数。

4 访问控制

外挂软件应用程序的访问控制功能应当从以下方面设计和实现:

1、外挂软件应用程序应当提供对软件功能和资源的访问控制功能，控制用户对应用软件系统各项功能、文件、数据等客体的访问。

2、访问控制的覆盖范围应当包括访问主体、客体及它们之间的操作。应当由授权主体配置访问控制策略，并严格限制默认账户的访问权限。

3、应当实现以软件功能和用户操作行为特征为基本粒度的访问控制。

4、基于用户的访问控制策略应当实现授予不同用户完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。应当禁止用户同时具有业务办理、系统管理、安全管理、审计管理中两种及以上功能，禁止用户同时具有业务申请、业务审批的权限或者通过系统逻辑禁止用户对自身发起的申请进行审核。

5、系统初始化默认用户应当按照最小授权原则，只授予系统运行所必需的初始化参数设置、管理部门和用户维护、权限管理等功能;

6、*采用基于角色的访问控制策略。

7、外挂软件应用程序应当根据警员和非警员身份信息，严格控制非警员身份人员允许访问的软件功能和资源。

8、“授权传播”指将授权的权力传播给其他用户，使其可以获得将指定客体的访问权限授予其他用户的权限。具有“授权传播”分级功能的外挂软件应用程序，获得“授权传播”的用户，并未获得访问指定客体的权限，仅可将授权传播给不包含其自身的其他用户，如需访问指定客体，需同时得到“访问授权”。

9、具有分级“授权传播”功能的应用软件系统，应对授权传播进行限制，对不可传播的授权进行明确定义，由系统自动检查并限制这些授权的传播。

10、*对分布式外挂软件应用程序，应当实行统一的访问控制安全策略，确保每一个场地的主、客体具有一致的安全属性，并执行相同的访问规则。

11、对重要数据的访问与重要进程的操作，采用客户端 IP 地址和用户绑定等技术实现客户端访问授权管理。

12、*提供对重要数据访问频率的控制，通过对过高访问频度的预警及阻断，加强对重要数据的安全管理。

13、服务端、客户端、数据库各层之间接口进行信息交互时，应对接口访问的授权进行确认，非授权的接口访问应视为攻击行为，记入安全事件日志。

14、*通过对主体、客体设置敏感级别标记，对用户访问敏感信息的行为进行控制。

5 安全日志及审计

外挂软件应用程序的安全审计功能应当从以下方面设计和实现:

1、外挂软件应用程序应对所有用户的重要行为（如用户登录、业务操作、重要数据查询）记录日志。

2、日志的内容应当包含用户标识、操作时间、来源、行为、

结果、关联数据及资源等信息。

3、提供基于用户的安全审计策略设置、审计日志存储和异常情况预警功能。

4、*提供应用程序运行状态监控、监控日志存储和异常情况预警功能。运行状态包括应用软件功能模块运行、版本升级、后台任务运行及主机系统资源使用等。

5、提供应用程序核心功能定义、核心功能操作审计、审计日志存储和异常情况预警功能。

6、具备数据异常情况告警功能。异常情况包括数据异常篡改、数据不一致等。

7、安全审计策略的设计应当与用户标识与鉴别、访问控制等安全功能的设计紧密结合，还应当对许可访问的行为制定安全审计策略，如用户高频访问、规定时段外访问、账户长期未使用、非常规业务的办理等。

8、安全审计信息应当采取加密存储、生成校验码或者其他安全存储措施，避免存储的安全审计日志被非法查看、修改或者删除。

9、安全审计日志的存储期限不得少于1年。

10、应当提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

11、按照公安部制定的公安信息系统应用日志安全审计相关规定，设计应用程序中用户操作行为和接口服务的日志格式，并

在调用公安交通管理综合应用平台等核心系统请求服务接口时将相关审计信息写入核心系统。

6 数据完整性和保密性

应当对在应用软件系统控制范围内存储和传输的用户数据，从以下方面设计和实现完整性、保密性保护:

1、通过使用数据校验码算法，生成源数据的校验码，在存储、传输及处理过程中对重要数据的完整性进行校验，防止关键数据被非法篡改。

2、在对重要数据完整性检测时，发现其完整性被破坏的，应当记入系统安全审计日志。在数据更新时，发现原有数据完整性被破坏的，应当拒绝数据更新操作。

3、应当采用加密技术对应用软件系统的重要数据、隐私信息进行加密，实现数据保密性保护，防止信息泄露。

4、*对外挂软件应用程序中使用的缓冲存储器及其他动态记录介质，通过在释放其使用权时对剩余信息进行删除等措施，确保不会由于动态记录介质中的剩余信息引起信息泄漏。

7*抗抵赖性

应当从以下方面设计和实现应用软件系统的抗抵赖:

1、抗原发抵赖：对于在网络环境进行数据交换的情况，通

过提供选择性原发证据，实现抗原发抵赖功能。

2、抗接收抵赖：对于在网络环境进行数据交换的情况，通过提供选择性接收证据，实现抗接收抵赖功能。

8 软件容错

应当对人机接口或者通信接口输入的数据格式、长度等进行严格的逻辑校验，确保输入数据符合应用软件的设定要求以及数据的准确性、完整性。

9 资源控制

资源控制应当符合以下要求：

1、应当具备自动结束会话功能。通信双方的一方在一段时间内未做响应时，另一方能自动结束会话。

2、应当具备对应用程序最大并发会话连接数进行限制的功能。

3、具备对单个用户账户的多重并发会话进行限制的功能。

4、*具备对一个时间段内指定重要业务操作数进行限制的功能，防止对重要业务和数据的高频访问。

5、*具备对应用软件服务水平降低到预先规定的最小值进行检测和报警的功能。

6、*按应用软件系统的功能优先级进行资源的管理和分配。

10 软件代码安全

应当从以下几个方面对应用软件代码安全进行设计:

1、用户界面提示的错误信息应当简洁、清晰，不应直接显示与系统底层代码相关的信息。如需作错误诊断的，可在展现时将错误代码信息加密，用户可提交开发人员，经解密后再进行故障诊断工作。

2、*采用代码混淆、自定义装载器等技术提高系统代码的安全性，避免代码被反编译。

3、系统控制数据，如口令、密钥、数据库连接参数等，不应当在未受保护的程序或者文档中以明文形式存储。