贵州省公安厅科技信息化委员会办公室发布

GZGA 001（1）-2016

贵州省公安信息化技术规范

2016-01-01实施

2016-01-01发布

贵州公安警务综合应用平台集成技术规范

第7部分：应用组件日志规范（试行）

1. 前 言

GGZGA/Z XX-2014《贵州公安警务综合应用平台集成技术规范》目前分为12个部分：

第1部分：总则（试行）

第2部分：应用组件集成规范（试行）

第3部分：统一用户，组织机构规范（试行）

第4部分：访问控制服务接口规范（CAS）（试行）

第5部分：应用组件时钟同步规范（试行）

第6部分：应用组件存储规范（试行）；   
第7部分：应用组件日志规范（试行）；

第8部分：消息中心服务接口规范（试行）

第9部分：信息服务总线接口规范（试行）

第10部分：数据中心服务接口规范（试行）

第11部分：警务综合应用平台集成规范（试行）

第12部分：平台服务接口规范（试行）

本部分为GZGA/Z XX-2015《贵州公安警务综合应用平台集成技术规范》 的第7部分。

本部分适用于贵州省公安警务综合应用平台集成建设工作。对于本部分未能涵盖的内容将依据本部分的编写原则对本部分内容进行扩充。

本部分文件由贵州省公安厅科技信息通信处提出。

本部分文件由贵州省公安厅科技信息通信处归口。

本部分委托贵州省公安厅科技信息通信处负责解释。

贵州公安警务综合应用平台集成技术规范

第7部分：应用组件日志规范

# 范围

本规范适用于贵州省警务综合应用平台，为各接入平台的应用系统的日志存储提供技术规范和指导。

# 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 25069-2010 信息安全技术术语

GB 11643-1999 公民身份证号码

GA607-2006 公安信息网络IP地址编码规范

GA380-2002 全国公安机关机构代码编制规则

公安信息系统应用安全审计技术规范（试行）

# 术语和定义、缩略语

* 应用安全审计

对公安应用系统/资源库/组件的用户操作行为和接口服务进行监测、信息采集和存储，以备倒查追踪。

* 登录

用户通过某种认证后，进入应用组件的事件。

* 查询

用户登录到应用系统后，输入关键字查询应用组件信息资源的事件。

* 新增

用户登录到应用组件后，添加信息资源的事件。

* 删除

用户登录到应用组件后，清除已有信息资源的事件。

* 修改

用户登录到应用组件后，变更已有信息资源的事件。

# 日志存储规范

## 日志存储格式

日志数据包括登录、查询、新增、删除、修改、接口服务这六类用户操作行为的日志，应用组件的日志数据统一采用UTF-8字符集记录和存储，并向警务综合应用平台报送日志数据，可以统一归纳为以下三类日志数据进行存储。

### 登录日志

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **字段类型** | **长度** | **描述** | **参考标准** |
| 1 | 用户身份证号 | 字符型 | 18字节 | 用户身份证号 | 《公民身份证号码》 |
| 2 | 用户警号 | 字符型 | 6字节 | 用户警号 |  |
| 3 | 单位名称 | 可变长  字符型 | --- | 使用应用系统/资源库用户的单位名称 |  |
| 4 | 单位机构代码 | 字符型 | 12字节 | 使用应用系统/资源库用户的单位名称的组织机构代码 | 《全国公安机关机构代码编制规则》 |
| 5 | 用户名 | 可变长  字符型 | --- | 登录应用系统/资源库提供的用户名称 |  |
| 6 | 登录日期时间 | 日期时间型 | 8字节 | 登录时间，如2014/04/05 10:10:15 |  |
| 7 | 退出日期时间 | 日期时间型 | 8字节 | 退出时间，如2014/04/05 11:10:15 |  |
| 8 | 终端标识 | 可变长  字符型 | --- | 终端标识包括两类：IP地址和硬件序列号，通过公安网接入的终端，其终端标识为IP地址，如10.2.66.57；通过移动警务接入的终端，其终端标识为硬件序列号。 | 《公安信息网络IP地址编码规范》 |
| 9 | 登录结果 | 布尔型 | 1字节 | 用户登录的结果记录，包括成功/失败。 |  |

### 操作日志

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **字段类型** | **长度** | **描述** | **参考标准** |
| 1 | 用户身份证号 | 字符型 | 18字节 | 用户身份证号 | 《公民身份证号码》 |
| 2 | 用户警号 | 字符型 | 6字节 | 用户警号 |  |
| 3 | 单位名称 | 可变长  字符型 | --- | 使用应用系统/资源库用户的单位名称 |  |
| 4 | 单位机构代码 | 字符型 | 12字节 | 使用应用系统/资源库用户的单位名称的组织机构代码 | 《全国公安机关机构代码编制规则》 |
| 5 | 用户名 | 可变长  字符型 | --- | 登录应用系统/资源库提供的用户名称 |  |
| 6 | 终端标识 | 可变长  字符型 | --- | 终端标识包括两类：IP地址和硬件序列号，通过公安网接入的终端，其终端标识为IP地址，如10.2.66.57；通过移动警务接入的终端，其终端标识为硬件序列号。 | 《公安信息网络IP地址编码规范》 |
| 7 | 操作日期时间 | 日期时间型 | 8字节 | 用户操作时间，如2014/04/05 10:10:15 |  |
| 8 | 操作内容 | 可变长  字符型 | --- | 用于记录用户操作调用的具体SQL |  |
| 9 | 操作反馈 | 可变长  字符型 | --- | 记录有下一步操作的具体内容 |  |
| 10 | 操作描述 | 可变长  字符型 | --- | 针对用户操作调用的具体内容进行的中文描述 |  |
| 11 | 系统功能模块 | 可变长  字符型 | --- | 操作的系统功能模块名称，用于安全审计平台审计用字段 |  |
| 12 | 操作类型 | 字符型 | 1字节 | 包括查询、新增、删除、修改四个类型 |  |

### 服务日志

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **字段类型** | **长度** | **描述** | **参考标准** |
| 1 | 调用用户身份证号 | 字符型 | 18字节 | 用户身份证号 | 《公民身份证号码》 |
| 2 | 调用用户警号 | 字符型 | 6字节 | 用户警号 |  |
| 3 | 调用单位名称 | 可变长  字符型 | --- | 调用服务接口的单位名称 |  |
| 4 | 调用单位机构代码 | 字符型 | 12字节 | 调用服务接口用户的单位名称的组织机构代码 | 《全国公安机关机构代码编制规则》 |
| 5 | 调用用户名 | 可变长  字符型 | --- | 调用服务接口的用户名称 |  |
| 6 | 调用日期时间 | 日期时间型 | 8字节 | 调用服务接口时间，如2014/04/05 10:10:15 |  |
| 7 | 服务请求方名称 | 可变长  字符型 | --- | 服务请求方的应用系统或客户段名称，如贵州省派基系统 |  |
| 8 | 返回数据条目数 | 长整型 | 8字节 | 记录返回条目的数值 |  |
| 9 | 调用接口描述 | 可变长  字符型 | --- | 对调用的服务接口进行的描述 |  |
| 10 | 调用参数记录 | 可变长  字符型 | --- | 记录调用服务接口的参数和参数值 |  |
| 11 | 调用结果 | 布尔型 | 1字节 | 服务接口调用的结果记录，包括成功/失败 |  |

## 日志存储要求

### 数据完备性

为了便于安全审计平台的日志审计，应用系统6类操作的日志记录及字段内容完整性应达到100%。

### 数据一致性

为了便于安全审计平台的日志审计，应用系统存储的本地日志记录，应该同提供给安全审计平台的日志记录保持一致。

### 独立存放

应用系统应将日志按登录、查询、新增、修改、删除及接口服务6类不同操作分类存储，并与业务数据逻辑隔离。

## 日志备份

应用组件应定期对本地的日志记录进行备份，避免存储空间耗尽或遭受攻击，备份的周期不超过3个月。

## 日志归档

应用组件应提供对本地的日志记录进行归档，归档时间不少于1年，归档保存期内禁止日志删除。