**中国外汇交易中心**

**应用系统日志开发及管理规范（讨论稿）**

## ****第一章　总则****

### 第一条　概述

为规范中国外汇交易中心暨全国银行间同业拆借中心（以下称“交易中心”）应用系统日志开发及管理过程，进行精准日志实时监控、提高突发故障排错效率、提供丰富信息用于大数据分析、实现应用系统的安全审计功能，根据《中国人民银行软件开发规范》等文件规定，结合交易中心实际，制定应用系统日志开发管理规范（以下称“本规范”）。

本规范中所提各项要求，是交易中心应用系统应达到的基本要求，如有其他要求应以需求规格说明书形式另外提供。

### 第二条　适用范围

交易中心所有新建应用系统及新购应用软件须遵守本规范。对于在线及在建应用系统，如有条件改造，应遵守本规范。外购应用软件若不能遵守本规范的，应由软件供应方提出可行的技术方案，经技术开发部及工程运行部确认后实施。新建应用系统需通过工程运行部检测后方可上线。

### 第三条　用户范围

本规范用户范围为交易中心应用系统开发、运维过程中所涉及到的有关人员。遵循此约束也是外部开发商承接交易中心开发项目的前提条件。未经交易中心允许，不能将本规范拷贝、复制给第三方。

### 第四条　术语及定义

应用系统日志在本规范中指交易中心业务系统（各系统主管部门组织开发的应用程序及外购应用软件）在运行时生成的日志（包括服务器端及客户端日志），不包括操作系统、数据库等系统软件所生成的日志。

记录是日志中的一段内容，包括了应用程序运行时发生的一个事件的完整信息，一个记录对应一个事件。

字段是记录的组成部分。一个字段是组成事件的一个要素的描述。一个字段只包含一个要素。字段按顺序排列，组成一个记录。

换行符是一个或一组字符序列，表示一行的结束。日志文件的换行符保持统一。在Windows上，换行符是两个字符\r\n；在UNIX和Linux上，换行符是一个字符\n。

分隔符由一个字符组成，用于区分相邻字段。分隔符在应用日志中保持统一，且避免与字段内容冲突。分隔符一般可使用“|”等可打印字符。如果有字段的值为空，则将前后两个分隔符相连，以保证每个字段在记录中相对位置固定。

## ****第二章　通用要求****

### 第五条　日志分类

应用系统日志分为业务日志和应用日志。

业务日志是用户对系统进行业务操作的日志，包括但不限于业务登录及退出相关操作、交易指令相关操作、基础数据维护相关操作、各类业务处理及查询相关操作、数据导出操作等。业务日志记录范围一般由需求规格说明书指定。

应用日志是与应用系统运行维护有关的日志，包括但不限于程序启动和停止、系统间互联相关事件、服务调用及消息处理相关事件等。

### 第六条　日志应具备安全审计功能

应用系统应提供覆盖到每个用户的安全审计功能，对重要安全事件（包括用户变更、用户权限变更内容或变更操作、场务用户查询机构交易记录等敏感数据的操作，等等）进行审计；应保证无法删除、修改或覆盖审计记录。

审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等[[1]](#footnote-0)。

对于信息安全等保级别在三级以上的系统，还应保证无法单独中断审计进程，且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[[2]](#footnote-1)。

### 第七条　日志加密

日志整体不应加密保存，对于系统中的业务敏感信息禁止保存在日志中，可根据实际情况进行必要的加密或替换处理（如打印“\*\*\*”），避免被用户直接读取分析。同时禁止使用DEBUG以上级别打印敏感信息。部分极端敏感信息（如密码）禁止直接输出到日志。

## ****第三章　业务日志规范****

### 第八条　业务日志的内容

业务日志记录一般包含以下信息：序号、时间（记录到秒）、用户唯一标识、功能操作、操作内容[格式：动作（包括但不限于新增、删除、查询、修改、登录、签退、授权、数据导出）+业务内容描述]。

## ****第四章　应用日志规范****

### 第九条　文件命名

日志文件名称：<系统名称英文简写>-<进程服务名英文简写>-<YYYYmmdd>-<滚动序号(由0开始)>.log

例如：tbs-dqs-20190619-0.log

（实际内容不包括尖括号）

根据具体应用系统需求确定日志滚动方式：按日期滚动或按文件大小滚动，及单个日志文件大小限制等参数。

| **滚动方式** | **要求** |
| --- | --- |
| 按日期滚动 | 可配置日志是否按日期切换方式，默认配置为“是”。  切换时生成同名文件，原文件名后追加“.时间戳”,时间戳的格式是YYYYmmddHHMM（年月日时分）。  日志切换时，如果删除或移动了正在被监控的日志文件，则必须立即创建与原文件同名的新文件。 |
| 按文件大小滚动 | 单个日志文件大小限制可配置，默认配置为不超过100M。  当日志切换时，在原文件名后追加“-序号”形成存档文件，序号是切换后存档文件的编号，从1开始。  存档文件数量无限制。  日志切换时，如果删除或移动了正在被监控的日志文件，则必须立即创建与原文件同名的新文件。 |

无论采用何种滚动方式，日志滚动后，新的记录写入原日志文件。举例来说，日志名为a.log，滚动后出现新文件a-1.log，则新记录写入a.log而不是a-1.log。

### 第十条　文本编码要求

应用日志文件的编码应为UTF-8。

### 第十一条　日志记录的格式

以“|”作分隔符为例，每一条日志记录的格式是：

时间戳|严重级别|进程所在主机名|进程ID|线程ID|唯一标识|错误代码|文件名:代码行|日志内容

一个记录的总字节数（不包括换行符；一个中文字符占三个字节）不超过1000个字节。

### 第十二条　时间戳

应用日志记录的时间戳字段有如下要求：

1. 记录写入日志的时刻；

2. 时区统一，采用本地时区（GMT+8）；

3. 表示法格式统一：  
（实际内容不包括尖括号；下划线代表半角空格）  
<4位年份>-<2位月份>-<2位日期> <24小时制2位时>:<2位分>:<2位秒>.<6位微秒>\_<3位大写字母时区>

### 第十三条　严重级别

从高到低有5种级别可选择：FATAL、ERROR、WARN、INFO、DEBUG。级别使用场景的说明如下：

FATAL——致命，表示当该异常发生时，服务已不可用，系统管理员需要立即介入。这是最严重的日志级别，**必须慎用**。如果这种级别的记录经常出现，则说明该系统经常崩溃，不该投入生产环境。通常情况下，一个进程的生命周期中应该只记录一次FATAL级别的日志，即该进程遇到无法恢复的异常而退出。如果某个系统的子系统遇到了不可恢复的异常，那么该子系统的调用方也可以记录FATAL级别日志，以便通过日志报警提醒系统管理员修复。

ERROR——错误，该级别也需要马上被处理，但是紧急程度要低于FATAL级别。当ERROR异常发生时，已经影响了用户的正常访问。FATAL级别和ERROR级别的区别在于发生ERROR级别异常时，服务进程依然存在，但是不能提供正常功能。对于用户自己操作不当，如输入参数错误等，不应记为ERROR级别的。建议将FATAL与ERROR级应用日志单独输出到对应的error日志文件，方便运维发现重大系统问题。

WARN——警告，该级别表示系统可能出现问题、也可能没有，如网络的波动等。对于那些目前还不是异常，然而不及时处理也会变为异常的情况，也可用此级别。虽然不需要系统管理员马上处理，也是需要关注的。

INFO——信息，记录系统的正常运行状态，例如某个子系统的初始化，某个请求的成功执行等。通过查看该级别的日志，可以很快地对系统中出现的异常进行定位。

DEBUG——调试级别，记录了程序每一步的执行过程，可以准确定位是何种操作、何种参数、何种顺序导致了某种错误的发生；可以保证在不用重现错误的情况下，也可以通过该级别日志对问题进行诊断。

系统设计阶段应明确每一条记录的级别，不应记录无意义的、级别定义不精确的日志内容，以免导致监控系统错误报警。

### 第十四条　唯一标识

唯一标识分为“业务唯一标识”和“技术唯一标识”，“唯一标识”在不特别说明的情况下指技术唯一标识。

“业务唯一标识”在业务日志中使用，表示一个交易的流水号或者业务代码，可以跨系统。业务唯一标识包含数字、字母和下划线三类字符。如果业务自身没有定义此类标识，则用统一的代码表示。

“技术唯一标识”（如TraceID）在应用日志中使用，一般在单个系统内使用，也可以跨系统。使用TraceID可以跟踪完整的调用链，整个调用链是一棵树形结构，TraceID的传递涉及到主干与支干，进程内与进程外。

### 第十五条　错误代码

错误代码在应用日志中使用。错误代码定义参考错误代码设计规范中相关内容。格式上，错误代码没有空格，前后各有一个半角空格。

## 第四章　应用日志运维管理规范

### 第十六条　监控报警触发条件

只能根据严重级别，而不是记录中的主体内容来设计报警触发条件。如果要求包含特定内容的记录不要触发报警，应降低其严重级别。反之，应提高其严重级别。

### 第十七条　生产环境日志级别

生产环境的日志级别为INFO及以上级别，关闭DEBUG级别。以下特殊情况可暂时允许开启DEBUG级别：

新业务系统上线（不包括版本升级）一个月内，生产环境的日志级别可开启DEBUG。此阶段要观察日志内容，分析业务系统运行状况。日志内容不断调整，删除无用记录，重要内容提高级别。上线满一个月，日志关闭DEBUG级别。

如果遇到只有在生产环境发生、无法在开发和模拟环境重现的故障，一定要在生产环境进行调试，则由相关部门向工程运行部提出申请，工程运行部评估同意后，通过变更，开启DEBUG级别。7个自然日之内，无论故障解决与否，都要关闭DEBUG级别。

### 第十八条　日志文件权限

系统设计阶段应根据具体需求在应用系统中增加日志防篡改功能。在操作系统用户权限分配及文件属性默认配置时，须设置同组及其他用户对日志文件有只读权限，即文件权限位不高于644，日志文件完整路径上所有目录的权限位不高于751。

### **第十九条**　**日志的保存与备份**

日志的保存时间应满足审计要求，如审计部门、业务部门未有明确规定，日志至少保存3个月，一般保存6个月为宜。用于抗抵赖性的日志，应永久保留，以便事后审计核查。应在运维手册中说明业务日志历史日志的存放目录、名称、备份周期[[3]](#footnote-2)。

### 第二十条　日志获取

对于服务器端日志，可直接在生产环境进行阅读及分析；对于客户端日志，应根据实际需求提出客户端日志获取需求，需求可包括但不限于本地日志分析、日志上传等功能；对于已经备份的日志，须首先在非生产环境的服务器上进行恢复。服务器端日志文件如需导出至其他环境（模拟环境除外），应填写《生产系统历史数据申请/使用申请表》和《生产运行系统服务/变更操作申请表》。日志使用后须按照交易中心保密相关制度尽快销毁。

### 第二十一条　第三方工具

对于应用系统集成的第三方工具，在可以配置日志格式时，需与本规范对齐，便于统一监控。

## 第五章　附则

### 第二十二条 解释

本规范由技术开发部及工程运行部负责解释。

### 第二十三条 施行

本规范自印发之日起施行。原《中国外汇交易中心应用系统日志开发及管理规范（试行）》（中汇交综〔2013〕2号）同时废止。

1. 《人民银行信息系统信息安全等级保护实施指引》 4.1.1.4小节 [↑](#footnote-ref-0)
2. 《人民银行信息系统信息安全等级保护实施指引》 4.2.1.4小节 [↑](#footnote-ref-1)
3. 《中国人民银行软件开发规范》 10.2.1小节 [↑](#footnote-ref-2)