# ****SMG信息传达系统需求说明书****

## ****项目概述****

总编室目前依靠口传的模式进行消息传递，模式相对落后且过程比较难追溯。根据前期调研，急需建设一套内部的SMG信息传达系统，为集团总编室提供安全、高效的宣传信息传达服务。并可支持多终端实时通讯，确保信息传达的时效性与安全性。建设目标如下：

* 满足内部信息下发即时通讯需求，确保信息传达的及时性、准确性和可追溯性
* 支持点对点、群发等模式进行信息发送，并消息通知
* 实现多平台（PC端和移动端）的统一管理，移动端接入“SMG纵横”
* 实现应用层面、系统层面、网络层面的数据安全性和保密性

## ****详细功能需求****

### 移动端

#### 入口

移动端将集成于企业微信，在企业微信可直接进入SMG信息传达系统。

#### 全部



进入SMG信息传达系统，底部导航共有全部、未读、发消息、群组、统计五个主要功能。

全部页面展示历史接收到的全部消息。消息列表展示发送用户头像、消息的标题、发送的时间。

##### 用户名片

用户头像由系统根据用户名直接生成。点击头像查看用户属性卡片，展示用户名、部门、联系方式如下：



##### 消息状态

**未读**：代表消息未读，且消息的生命周期还未到删除的时间。点击消息后可查看内容。

**已读**：代表消息已读。点击已读消息后不可查看内容，并在页面展示最终阅后即删除的时间。

**逾期**：代表消息未读，但消息的生命周期已超过未读删除的时间。点击消息后不可查看内容，并提示最终未读删除的时间。

#### 未读

未读整体逻辑和全部页面一致，只是对全部消息内容的筛选，筛选出用户未读的消息。

##### 未读消息数量提示

未读的底部导航图标需要红点展示未读且可读消息的数量(未读-已删除的消息数量不计入在内)。

##### 阅后即删除逻辑

用户点击**未读**的消息后，直接进入消息内容页面。

消息内容仅可查看一次。查看完成返回列表页，消息变为**已读**状态，再次进入消息页面，消息页面提示阅后即删除。

进入**未读**消息页面后就会开始阅后即删除倒计时，时间耗尽后，消息也会转换为**已读**状态，不再展示消息内容，提示阅后即删除。

阅后即删除的时间可由后台配置。

若用户的未读消息，在超过后台设置的未读删除时间后，将自动转换为**逾期**状态。

##### 文本消息

文本消息展示重要消息标题、发送人名称、发送时间。

##### 文本消息字号调整

文本内容的文字大小默认值按后台设置的大小展示，同时支持调整字体大小，最小8号字，最大20号字。调整到最大值时A+按钮置灰，调整到最小值时，A-按钮置灰。

##### 图片消息



图片消息最多展示9张图片

##### 语音消息



语音消息需要可以拖动语音播放的进度条反复播放。

##### 文件消息（PDF）



文件消息直接展示文件名和文件预览内容。

##### 消息转发

消息转发的操作受到两个方面的影响：

* 用户是否移动端发消息的权限

若用户没有发消息的权限，则也不可转发。转发按钮不显示。

* 消息的转发时间限制

后台可设置消息的可转发时间，若消息发送后的计时超过了消息的可转发时间，则用户不可转发该条消息。转发按钮不显示。

转发消息时，文本类型的消息可修改标题和内容，其他类型的消息仅可修改标题。

#### 发消息

发消息页面支持发送文本、图片、语音、文件四种类型的消息。全部消息类型都需要输入消息标题，并选择接收人。

标题：文本框输入，最多支持输入20个字。

接收人：点击接收人进入选择接收人页面。该页面展示当前用户有发消息的群组。并展示群组下的所有成员。用户可选择发送消息的成员，选择用户过多时，页面需缩略展示选择的接收人。

##### 发送文本消息

发送文本消息限制2000个中文字符。

##### 发送图片消息

图片消息最多支持上传9张图片，支持格式为：png、jpg、bmp、jpeg。

##### 发送文件消息

文件消息单次只支持上传一个文件，格式要求为PDF，大小小于100MB.

##### 保存草稿

发消息页面下方展示保存草稿按钮，点击后可保存当前页面输入的内容，上传服务器。之后每次打开，将展示保存的草稿内容。

保存草稿仅可以保存一种消息内容。仅会保存当前内容的消息，若图片和文字都有内容，当前页面停留在文字页面，则仅会保存标题、接收人及文字内容。

若草稿超过后台设置的草稿保留时间，则清除草稿内容。

##### 交互提示

**切换消息类型提示**

若切换消息类型时，用户已经编辑了内容，则需提示用户以下消息：

若未保存草稿，切换消息类型后当前已编辑内容将丢失。是否确认切换？

**发送消息成功提示**

发送消息后，需提示用户已发送了哪些用户，提示消息示例：

消息已发送给XXX、XXX、ZZ。

**保存草稿提示**

您已成功保存草稿。

#### 群组

##### 创建群组

群组页面的搜索框可按群组名称搜索。

点击+可选择联系人创建群组，列表的联系人会展示联系人的部门岗位，也可点击组织架构，勾选具体某个部门下的用户创建群组。

联系人列表及组织架构都支持人名搜索

##### 群组资料

点击群组列表的群组，可直接进入群组的资料页面。群主可修改群名称、添加/移除成员、设置发消息权限、解散群组。 普通成员仅可查看不可编辑。

##### 设置群组名称

群组名称可以修改

##### 添加群成员

群成员可查看全部的群组用户，点击添加可选择联系人加入群聊

##### 移除群成员

有权限人员可以删除群组成员

##### 设置发消息权限

被赋予发送重要消息权限的用户，可以在群组功能中看到本群组，并可在发送/转发消息时，选择该群组的群成员。

##### 解散群组

点击解散群组按钮，弹窗确认后可解散当前群组。

#### 统计

统计页面展示当前用户发送过的消息，并展示消息传播覆盖的去重总人数、去重已读人数、去重未读人数及转发次数。

用户可在此页面撤回或转发消息。

##### 统计明细

统计明细页展示重要消息的标题、发送人、发送时间，若消息是转发的消息，还要展示转发自哪个用户。

明细页面展示统计数据、我发送的、我转发的阅读明细数据。

**统计数据**：和外部列表展示一样，展示消息传播覆盖的去重总人数、去重已读人数、去重未读人数及转发次数。

**我发送的**：展示当前用户直接发送用户的已读/未读情况。 已未读读用户都展示头像、名称、部门-岗位，已读用户多展示一个阅读时间。

**被转发的**：展示经由当前用户发送的用户转发的已读/未读情况。 已未读读用户都展示头像、名称、部门-岗位，已读用户多展示阅读时间和阅读的消息来自于哪个用户转发的。

#### 消息生命周期控制

由于信息安全性的需求，对于下发的消息有以下功能：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 场景 | 触发条件 | 系统动作 |
| 1 | 阅后即删除 | 用户打开信息 | 启动倒计时（默认5分钟，时间后台可配置） |
| 2 | 未读删除 | 发送后24小时（时间后台可配置） | 自动删除 |
| 3 | 紧急撤回 | 发送方操作 | 立即移除未读消息，已读人员需要弹窗提示 |
| 4 | 动态水印 | 所有页面 | 查看消息人员工号、姓名 |

#### 内容支持格式

* 语音消息：支持最长5分钟（暂定）录制，自动降噪优化
* 文字信息：限2000中文字符
* 文件：pdf文件，大小限制100M以内

#### 阅读状态追踪

消息发送人员可在发送管理界面查看已读人员信息和未读人员信息，参考模式如下：

宣传指令：XXXXXXX （发送时间：2025-01-01)

已读人员（2人）：张三（2025年3月2日09:30）、李四（2025年3月2日10:15）

未读人员（2人）：王五、赵六

转发的消息，未读用户也要一起展示：若A群发的消息，A群的群员转发给B群，B群的群员转发给C群。则A群的转发人可见ABC群全部的已未读用户，B群转发人可见BC群的已未读用户，C群转发人可见C群的已未读用户。

### 后台管理

#### 人员管理

人员管理按部门组织架构树展示人员的基本信息（工号、姓名、部门、岗位、角色），可启用禁用。支持对接UD同步人员信息。

#### 角色管理

角色管理可配置系统中的角色。可设置角色的菜单权限和移动端权限。菜单权限控制用户可见的后台功能菜单，移动端权限控制移动端相关的权限内容。

**移动端权限有：**

发消息：控制移动端是否展示发消息页面底部导航。

群组：控制移动端是否展示群组页面底部导航。

创建群组：控制移动端是否展示创建群组按钮。

全部组织架构：控制移动端创建群组/添加成员时能否看到全部组织架构。

本部门及以下：控制移动端创建群组/添加成员时能否看到本部门及以下组织架构。

统计：控制移动端是否展示统计页面底部导航。

#### 部门管理

部门增删改查。

#### 群组管理

开放给管理员在后台给群组添加和移除成员的功能。

#### 统计

统计功能记录用户发送的消息记录，展示重要消息标题，可点击查看内容查看消息详情，也可点击阅读状态查看消息的已读名单及阅读明细。

##### 查看内容

查看内容展示消息类型、发送人、接收人、发送时间、发送方式、转发自、标题内容、源标题、源内容。

其中“转发自”字段仅发送方式为转发时有值，“源标题”、“源内容”，仅发送方式为转发时展示。

消息类型为文本时，且发送方式为转发时，需要对比标题和内容相较于源标题、内容产生了哪些变化。

消息类型为其他类型时，且发送方式为转发时，仅需对比标题变化。

##### 阅读状态

阅读状态展示统计数据、阅读名单及阅读明细。

**统计数据**

展示消息传播覆盖的去重总人数、去重已读人数、去重未读人数及转发次数。

**阅读名单**

* 展示去重的已读/未读用户名单，展示用户的姓名、已读/未读状态、阅读时间。 已读用户默认排序靠前。
* 若同一个用户同时有已读和未读的记录，则记录此用户为已读。
* 列表支持按已读/未读状态筛选。
* 列表支持导出。

**阅读明细**

* 展示全量的直接发送接收人及转发接收人，并记录这些接收人的阅读状态，消息的发送人，及传播路径、阅读时间。
* 列表为非去重数据，若有多个用户转发给同一个接受人，则此接收人可以重复出现。
* 列表支持按已读/未读状态筛选。
* 列表支持导出。

##### 消息内容导出

统计列表左上角展示导出按钮，导出后可进入内容导出流程。每次导出，需要设置导出的截止时间，并获取系统管理员的手机验证码，验证后，方可导出数据。

导出的时间范围默认是上一次设置的截止时间到本次设置的截止时间。

##### 导出日志及数据清除

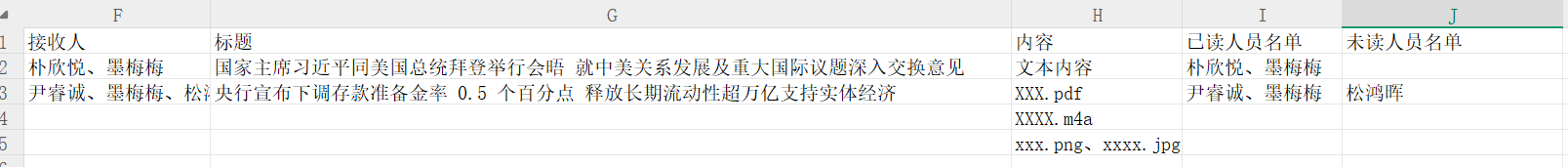
点击导出日志按钮，可查看历史导出的记录，展示导出人，导出时间，及导出内容的时间范围。

导出时间范围的开始时间默认是上一次导出的结束时间。

已导出的记录，可点击清除已导出数据，清除操作需要二次确认。清除后，将从数据库层面彻底删除已导出的消息内容标题、及相关的阅读数据。

##### 导出文件结构

如图所示，导出需一次导出三个文件，分别是消息记录导出、阅读状态导出、消息附件导出。其中消息记录导出字段结构如下：



#### 参数设置

**参数设置可设置如下内容：**

阅后即删除时间、未读删除时间、消息撤回时间、可转发时间、消息保留时间、消息草稿保留时间、文本信息内容字体大小、IP白名单列表。

## ****与其他平台的对接****

* PC端与统一认证对接
* PC端与UD系统对接
* 移动端接入“SMG纵横”

## ****安全架构需求****

### 需求概述

本SMG信息传达系统安全要求高，针对 SMG 信息传达系统的业务特性，围绕消息从生成、发送、传输、接收到删除的完整生命周期，构建多维度、多层级的安全防护体系。方案覆盖移动端、管理端，依托 Nginx 负载均衡服务器、DMCDM 国产达梦缓存数据库、DM8 国产达梦关系型数据库、文件存储系统等核心组件，实现从接入认证、传输加密、存储保护、权限控制到审计追溯的全链路安全管控。

### 安全架构设计

#### 网络接入与传输安全

* **接入层防护**：移动端、管理端接入时，管理端采用 “认证 + IP 白名单限制”，移动端采用 “认证 + 会话超时注销”，经 Nginx 转发，Nginx 配置国密套件（TLSv1.3、ECDHE - SM4 - WITH - SM4 - SHA3 ），保障传输链路加密，防止数据窃听、篡改 。
* **应用拦截器**：部署 IP 白名单拦截，仅允许合规源 IP 访问管理端；用户身份认证采用密码认证；含合法请求校验（校验 token 有效性、防重放 ）；功能权限拦截（依据用户角色，限制创建、编辑等操作 ）；数据权限拦截（按用户权限，限制数据查询、下载范围 ）；操作审计记录（记录操作行为、时间、用户，用于事后追溯 ）。

#### 数据存储安全

* DMCDM 存储（国产达梦缓存数据库）：敏感配置加密存储，数据同步时采用国密 SM4 加密，确保数据传输、存储安全 。
* DM8 数据库（国产达梦数据库）：敏感字段（如消息标题、消息内容）加密存储（国密 SM4 ），支持数据完整性校验，防止数据篡改、泄露 。
* 文件存储：图片、语音、pdf文件加密存储（国密 SM4 ），提供文件访问权限管控，防止越权获取 。

#### 消息生命周期安全管控

1. **发送侧安全控制**：执行权限边界拦截（按角色权限，阻断未授权消息发送 ）、消息标记（消息自动绑定 “阅后即删除” 等策略 ）、内容格式校验（管控文件格式、附件大小 ） 。
2. **传输中安全保障**

* 双层加密机制：传输层使用国密 TLSv1.3 协议，实现端到端加密；应用层对消息体使用 SM4 算法的 GCM 模式加密，同时生成 256 位的消息认证码（MAC），确保数据机密性和完整性。加密流程如下：

1. 客户端生成随机 SM4 密钥 K 和初始化向量 IV
2. 使用 K 和 IV 加密消息体，得到密文 C
3. 使用 K 对 C 和时间戳 T 生成 MAC 值
4. 使用服务器公钥（SM2 算法）加密 K 和 IV，得到 EKIV
5. 发送数据格式：EKIV + C + MAC + T。

* 防篡改校验：接收端收到消息后，首先验证时间戳 T 的有效性（允许 5 分钟误差），然后使用私钥解密 EKIV 得到 K 和 IV，用 K 对 C 解密得到明文，再用 K 对解密后的明文和 T 生成新的 MAC 值，与接收到的 MAC 值比对，一致则通过校验。

1. **接收侧安全处理**

* 二次身份校验：接收端收到消息后，首先通过消息头中的发送方证书（基于 SM2 算法的数字证书）验证发送方身份，证书包含发送方公钥、单位信息、有效期等，由系统根证书颁发机构（CA）签名。验证失败的消息直接丢弃并记录告警。
* 动态水印技术：消息展示时，在界面层叠加半透明动态水印，内容包含查看者工号、姓名查看时间，防止截图识别。
* 阅后即删除实现：重要消息阅读后启动 5 分钟倒计时，倒计时结束后通过前端自动屏蔽掉不让用户查看。
* 防截屏录屏措施：安卓移动端限制用户截屏行为，IOS移动端记录截屏行为。

#### 权限管理设计

* **后台管理员**：具备人员、角色、部门、岗位、标签、群组管理权限，可配置系统参数、查看消息日志，实现全局权限管控 。
* **总编室权限**：支持创建群组、发送 / 转发消息，设置群内消息权限，查看消息阅读状态，聚焦业务核心操作 。
* **普通用户**：可接收消息，保障基础功能使用，限制高风险操作 。

#### 消息策略配置

1. **全流程涉及内容安全策略的参数详解**

* 阅后即删除（5 分钟）：基于 ISO 27001 中对敏感信息处理的要求，结合SMG信息传达系统实际场景，5 分钟足以完成正常阅读，超时自动删除可有效防止消息被截图或转发。技术实现上，通过消息头中的过期时间戳和前端定时器控制，时间戳采用 UTC 格式，精确到秒。
* 未读超时（12 小时）：考虑到消息的时效性，12 小时未读的消息自动标记为过期，释放存储资源，同时避免重要消息被遗漏。系统每天凌晨 1 点对所有超过 12 小时未读的消息执行批量过期处理，并生成未读报告发送给发送者。
* 消息撤回（2 小时）：2 小时内允许撤回已发送消息，基于以下考虑：编辑可能在消息发出后发现内容错误或敏感信息泄露，2 小时内撤回可最大限度减少影响。撤回机制采用 "标记删除" 方式，服务器保留撤回记录，包含撤回时间、操作人等信息。
* 可转发时间（2 小时）：限制消息在发送后 2 小时内可转发，防止非授权扩散。转发时自动携带原消息的敏感度标记和转发记录，形成完整的消息链，便于追溯。

1. **消息留存策略与合规性**

* 消息留存 1 天：消息留存一定时间用于审计和追溯。留存内容包括消息标题、发送时间、发送人、接收人等元数据，消息内容采用 SM4 加密存储，仅在发生安全事件时由管理员查看访问。
* 操作留痕机制：所有用户操作（包括消息发送、转发、删除、权限变更等）均记录完整日志

1. **IP 白名单策略**：限定管理端访问范围，仅允许总编室内网、指定安全 IP 接入，拦截非法访问，守护核心权限、策略数据安全 。

### 安全保障与审计

* **应急响应**：建立安全事件应急预案，涵盖数据泄露、系统攻击等场景，明确响应流程、责任分工，定期演练，保障快速处置。
* **审计机制**：依托操作日志、发送记录，定期开展安全审计，检查权限合规性、数据完整性、策略执行情况，输出审计报告，持续优化安全体系。

## ****非功能性需求****

### 性能指标

* 消息投递延迟：<3秒（95%场景）
* 并发支持：≥100人同时在线

### 兼容性要求

* 浏览器：Chrome 100+、Edge 100+、Safari 15+
* 移动端：Android 10+/iOS 14+

### 其他要求

* 系统上线验收前，需要通过第三方公司的代码审计，第三方公司代码审计费用不包含在本项目中。
* 本系统必须能够运行在达梦数据库、银河麒麟操作系统、服务器海光CPU基础环境上。