

T-UPA0006-2022

V1.0.0(2022-3)

办公即时通信软件 第1部分：安全要求和测试方法

Security Requirements and Testing Methods for Office Instant Messaging Software



Unified Push Alliance
统一推送联盟

目 次

目 次.....	I
前 言.....	II
1 范围.....	3
2 规范性引用文件.....	3
3 基本安全架构.....	3
4 应用APP安全要求	3
5 认证安全要求.....	4
6 应用层安全要求.....	5
7 通信安全要求.....	6
8 应用APP安全测试方法	7
9 认证安全测试方法.....	10
10 应用层安全测试方法.....	14
11 通信安全测试方法.....	18

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分 标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由统一推送联盟提出并归口。

本文件起草单位：中国信息通信研究院、海比研究院、广州腾讯科技有限公司、钉钉科技有限公司、北京飞书科技有限公司、北京北信源软件股份有限公司、杭州网易智企科技有限公司、上海奇夜语网络科技有限公司、科大讯飞股份有限公司、中兴通讯股份有限公司、中国联通中讯邮电咨询设计院、北京百度网讯科技有限公司、厦门亿联网络技术股份有限公司、深圳市蓝凌软件股份有限公司、蓝信移动（北京）科技有限公司、北京云中融信网络科技有限公司、北京易掌云峰科技有限公司、深圳云之家网络有限公司、北京容联易通信息技术有限公司、北卡科技有限公司。

本文件主要起草人：李玮、王景尧、吴荻、曹开彬、冯艺卓、郑如彬、徐永太、陈凯、高景强、代威、马建坤、黄天宁、张琪琪、李卓然、李华明、汪广毓、张雷、王宇晓、高曦、宋萌、蒋国辉、杨大郁、张腾、周森、徐杭生、廖百成、马虎、童振宁、宋景豪、张小燕、吕亚敏、魏鹏刚、唐珂、王亮、李蔚然、陈浩然、张云平、童圣杰、苏霄雅、柯剑峰、张建光、谷恒召、裴利杰、刘建军、范强、符宁、于磊婷、徐衡、张欣、李礼、牟博松、许春耀。

办公即时通信软件 第1部分：安全要求和测试方法

1 范围

本文件规定了办公即时通信软件的总体安全要求和测试方法。

本文件适用办公即时通信软件的开发者、提供商及专业测评机构开展安全测试工作，为提升办公即时通信软件安全水平、强化测试能力、健全技术手段提供指引和依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

GB/T25000.10—2016系统与软件工程系统与软件质量要求和评价(SQuaRE)第10部分：系统与软件质量模型

GB/T25000.51—2016系统与软件工程系统与软件质量要求和评价(SQuaRE)第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则

GB/T18336.1—2008信息技术安全技术信息技术安全性评估准则第1部分：简介和一般模型

GB/T22240—2008信息安全技术信息系统安全等级保护定级指南

GB/T28452—2012信息安全技术软件系统通用安全技术要求

3 基本安全架构

办公即时通信软件的基本安全架构如图1所示，其面临的主要安全风险存在于移动终端、通信传输、数据安全等方面，基于对办公即时通信软件的安全风险分析，办公即时通信系统的安全技术框架应包括应用APP安全、认证安全、应用层安全、通信安全。

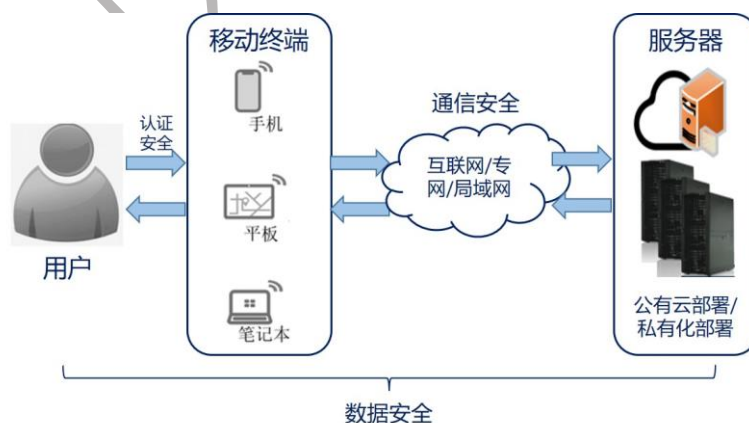


图1 办公即时通信软件安全基本架构

4 应用 APP 安全要求

4.1 代码安全

办公即时通信软件应保证应用 APP 代码安全性，通过完整的 SDL 流程，保证在人员培训、需求分析、代码开发、应用测试、项目发布、应急响应等安全开发生命周期中的应用代码安全。基本的应用 APP 代码安全包括但不限于：

- a) 敏感数据防泄漏检测：代码开发中应保证敏感信息不被从应用 APP 中泄漏；
- b) 应用完整性检测：代码开发中应对应用 APP 的完整性进行校验，避免重打包，恶意代码注入等；
- c) 密码学安全：代码开发中应该使用无已知安全漏洞的密码学组件，并按照相关规范正确配置。

4.2 环境安全

办公即时通信软件宜具备应用客户端运行时环境安全检测能力，保证能够依据应用 APP 所处的硬件环境，系统环境，网络环境等因素进行针对性的安全策略调整，从而保证应用 APP 运行在可信环境中。环境安全检测包括但不限于

- a) Root、越狱检测；（可选）
- b) 地理位置检测；（可选）
- c) 运行环境检测。（可选）

4.3 供应链安全

办公即时通信软件应确保应用 APP 所依赖的供应链组件安全性。供应链安全检测包括但不限于：

- a) 对引入的供应链组件进行检测，当前版本无已知高危漏洞。
- b) 正确配置供应链组件，避免因错误配置产生的问题。

4.4 应用加固

办公即时通讯软件宜具备必要的安全加固机制以保障应用 APP 不被逆向破解。应用加固方式包括但不限于：

- a) 代码混淆：批量替换变量，函数，类的名称为无意义命名，重写代码中部分执行逻辑，使其变成功能等价，但更难理解的形式；（可选）
- b) 核心加密：对核心的代码逻辑需要进行加密加固，使得静态分析难以还原和理解；（可选）
- c) 数据库加密：对本地保存用户信息和数据的数据库，需要进行加密保存，一机一账号一密。（可选）

5 认证安全要求

5.1 登录安全

5.1.1 身份标识

- a) 应根据不同的业务需求对用户进行标识，确保所标识用户在本系统生命周期内的唯一性，并与安全审计相关联。
- b) 应对用户标识信息进行管理和维护，确保其不被非授权的访问、修改和删除。

5.1.2 设备标识

- a) 应对连接到系统的终端设备，在将其接入到系统前先进行标识。应对设备标识信息进行管理、维护，确保其不被非授权的访问、修改或删除。
- b) 应对新连接到系统的设备与用户标识进行关联，并对设备进行全生命周期管理。

5.1.3 环境识别

- a) 宜对终端设备所处的网络环境、系统环境进行识别、记录，并根据安全要求制定对应的管控策略。（可选）

5.1.4 身份鉴别

- a) 在用户访问系统前，应对用户身份进行鉴别。宜采用多因素认证方法对用户身份进行鉴别。身份鉴别方式应支持两种或两种以上，如静态口令、短信验证码、动态口令、数字证书、生物特征等。
- b) 应对身份鉴别信息进行加密。

5.1.5 登录策略要求

- a) 根据组织的安全要求，可根据现实场景（如网络环境、系统环境、设备类型等）制定登录策略，进行登录控制。（可选）
- b) 宜对相同终端上的重复登录行为进行识别和管控。（可选）

5.2 权限

- a) 在访问业务资源前，应先对用户成功地进行身份鉴别，并能够根据用户相应的访问权限返回业务数据。
- b) 可采用已登录终端设备扫码授权的方式进行授权登陆。（可选）
- c) 应对已停用账号的访问权限进行控制。

5.3 错误锁定

- a) 应针对在规定时间内多次身份鉴别失败的用户进行锁定，在规定时间内进行解锁。
- b) 可对在规定时间内多次修改口令或找回口令的用户进行锁定，在规定时间内进行解锁。（可选）
- c) 在登录错误信息返回时，应采用模糊提示。

5.4 账号口令

- a) 应对口令复杂度进行控制，包括口令长度、字符组成等；避免使用含有账号信息的口令及常见口令。
- b) 可具有口令找回或口令重置的能力，并具备验证机制。（可选）
- c) 可对口令变更周期进行控制。（可选）
- d) 不应默认保存用户上次的账号及口令。
- e) 修改身份鉴别方式时，可验证原有身份鉴别方式。（可选）

6 应用层安全要求

6.1 通讯录管理

- a) 应支持组织架构可见性设置；支持隐藏敏感字段。
- b) 宜支持手机号安全查看审计，宜支持查看数量达到上限的提醒策略。（可选）

6.2 授权管理

- a) 宜支持分级制授权管理，指定组织节点分配分组管理员，实现集中管理、分层授权。（可选）

6.3 聊天申请

- a) 可支持对聊天权限的灵活控制，在触达不可见成员（如非好友非同事等）的场景下，可设置聊天申请权限。（可选）

6.4 敏感信息过滤

- a) 宜支持敏感信息过滤，管理员可在后台设置需要过滤掉的敏感信息。导入成功后，系统自动通过敏感信息匹配而进行信息拦截。（可选）

6.5 背景水印

- a) 应支持聊天显示水印。
- b) 可支持管理员配置在“聊天”、“通讯录”、“头像”、“邮件”、“网页”、“文件”等不同位置单独设置开、关水印功能。（可选）
- c) 水印显示的内容宜支持定制，如“姓名”、“手机号后四位”、“日期”、“邮箱”或者自定义字样。（可选）

6.6 消息撤回

- a) 应支持用户个人撤回指定时间内的消息。
- b) 可支持群管理员远程撤回。（可选）

6.7 消息防控

- a) 宜支持管理员在后台进行移动端安全管理设置，实现如消息防复制、防转发、防保存、防分享、防截屏、防录屏等功能。（可选）

6.8 消息推送

- a) 移动消息推送应支持不显示发信人和内容摘要。

6.9 群管理

- a) 应支持群成员邀请确认。
- b) 可支持群禁言，包括全部禁言、部分禁言等。（可选）
- c) 应支持群管理的权限设置。

6.10 音视频管控

- a) 应支持对音视频业务数据进行加密保护
- b) 可支持对音视频业务的接入人员进行管控。（可选）
- c) 可支持音视频业务的禁止录音、禁止录屏、禁止截图等。（可选）

6.11 动态密钥

- a) 可支持动态密钥认证，实现不联网或应用加固被破解场景下的敏感数据防泄漏。（可选）

6.12 检测与扫描接口

- a) 可支持病毒检测、敏感信息扫描接口。（可选）

7 通信安全要求

7.1 通信协议

- a) 传输层协议应采用TCP或UDP协议。
- b) 应用层协议应采用可扩展通讯和表示协议（XMPP）、即时消息和表示协议（IMPP）、即时消息协议（PRIM）、SIP即时消息和表示扩展协议（SIMPLE）、超文本传输安全协议（Https）等其中一种协议。
- c) 可支持私有协议，具备一定可读性和扩展性。（可选）

7.2 接入安全

7.2.1 接入权限安全

- a) 遵循最小权限原则，系统具备核心数据应做到仅开放当前接入用户可访问的范围。核心数据包括：消息、联系人数据、文件等企业用户私密数据。
- b) 系统的业务功能应做到按需开放，接入用户仅可以使用当前拥有权限的功能范围。

7.2.2 接入安全审计

- a) 宜具备对接入用户的审计能力。（可选）

7.3 传输安全

- a) 数据传输过程中应支持TLS 1.2（RFC 5246, 2008）及以上安全协议。
- b) 数据传输过程中可支持国密算法。（可选）
- c) 密钥应具备更新机制且支持多版本管理，确保不影响业务持续性。
- d) 公有云即时通信软件可支持端到端加密。（可选）

8 应用 APP 安全测试方法

8.1 代码安全

编号	5.1-a
安全要求	代码安全，无敏感数据泄漏问题。
预置条件	无
测试方法	a) 检查应用 APP 中是否有敏感信息（如密钥）硬编码。 b) 检查数据库是否明文存储。 c) 检查调试日志信息是否在正式版应用中去除。 d) 检查是否有敏感信息（如密钥）的明文传输。
预期结果	a) 应用 APP 中无敏感信息硬编码。 b) 数据库加密存储信息。 c) 正式版应用无调试日志信息。 d) 无敏感信息（如密钥）的明文传输。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.1-b
安全要求	代码安全，应用完整性保证。
预置条件	无

测试方法	a) 检查应用 APP 文件完整性。 b) 检查应用 APP 运行时内存完整性。
预期结果	a) 应用 APP 文件完整，未被重打包。 b) 应用 APP 运行时内存完整，未被注入恶意插件。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.1-c
安全要求	代码安全，密码学组件安全保证。
预置条件	无
测试方法	a) 检查应用 APP 使用的密码学组件是否含有高危漏洞。 b) 检查应用 APP 使用的密码学组件配置是否正确（如密钥长度足够）。
预期结果	a) 密码学组件版本无高危漏洞。 b) 密码学组件配置正确。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

8.2 环境安全

编号	5.2-a
安全要求	环境安全，Root、越狱检测。（可选）
预置条件	无
测试方法	a) 检查应用运行环境中是否被 Root、被越狱。
预期结果	a) 如运行环境被征 Root、越狱，应用能够给出提示。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.2-b
安全要求	环境安全，地理位置检测。（可选）
预置条件	无
测试方法	a) 检查应用运行环境中是否为虚拟定位。
预期结果	a) 应用运行环境为真实地理位置。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.2-c
安全要求	环境安全，运行环境检测。（可选）
预置条件	无
测试方法	a) 检查应用运行环境中是否为虚拟机、虚拟空间
预期结果	a) 应用运行环境为真实设备，或虚拟空间在白名单中。

判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合
------	---------------------------

8.3 供应链安全

编号	5.3-a
安全要求	供应链安全，供应链组件无漏洞。
预置条件	无
测试方法	a) 检查应用使用供应链组件版本，此版本是否含有高危漏洞。
预期结果	a) 供应链组件当前版本无高危漏洞。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.3-b
安全要求	供应链安全，供应链组件配置安全。
预置条件	无
测试方法	a) 检查应用是否按照规范配置供应链组件，避免因错误配置产生漏洞。
预期结果	a) 供应链组件配置正确。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

8.4 应用加固

编号	5.4-a
安全要求	应用加固，保证应用 APP 使用了代码混淆进行加固防御。（可选）
预置条件	无
测试方法	a) 检查应用 APP 是否使用代码混淆将变量、函数、类进行命名无意义化，程序流程复杂化。
预期结果	a) 应用 APP 使用了代码混淆。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.4-b
安全要求	应用加固，保证应用 APP 核心代码使用加密加固。（可选）
预置条件	无
测试方法	a) 检查应用 APP 核心代码是否使用加密技术
预期结果	a) 应用 APP 核心代码使用加密技术，反编译器无法正确解析
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	5.4-c
安全要求	应用加固，保证应用 APP 本地数据库进行加密存储。（可选）
预置条件	无
测试方法	a) 检查应用 APP 本地数据库是否加密存储，是否一机一密。
预期结果	a) 应用 APP 本地数据库进行了加密存储，并且一机一密。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

9 认证安全测试方法

9.1 登录安全

编号	6.1.1
安全要求	a) 应根据不同的业务需求对用户进行标识，确保所标识用户在本系统生命周期内的唯一性，并与安全审计相关联。 b) 应对用户标识信息进行管理和维护，确保其不被非授权的访问、修改和删除。
预置条件	无
测试方法	a) 使用重复的身份标识创建新的账号 b) 使用非授权账号对用户标识信息进行访问、修改和删除
预期结果	a) 系统应无法创建重复的账号 b) 应无法进行访问、修改和删除等操作
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.1.2
安全要求	a) 应对连接到系统的终端设备，在将其接入到系统前先进行标识。应对设备标识信息进行管理、维护，确保其不被非授权的访问、修改或删除。 b) 应对新连接到系统的设备与用户标识进行关联，并对设备进行全生命周期管理。
预置条件	无
测试方法	a) 检查终端设备是否被标识，并得到合理管理。 b) 检查设备是否与用户标识关联。
预期结果	a) 终端设备应被正确标识； b) 设备与用户标识正确关联。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.1.3
安全要求	宜对终端设备所处的网络环境、系统环境进行识别、记录，并根据安全要求制定对应的管控策略。（可选）
预置条件	无
测试方法	a) 检查是否支持对环境具备识别能力和管控策略。
预期结果	a) 应具备识别环境能力，并制定管控策略。

判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合
------	---------------------------

编号	6.1.4
安全要求	a) 在用户访问系统前，应对用户身份进行鉴别。宜采用多因素认证方法对用户身份进行鉴别。身份鉴别方式应支持两种或两种以上，如静态口令、短信验证码、动态口令、数字证书、生物特征等。 b) 应对身份鉴别信息进行加密。
预置条件	无
测试方法	a) 使用已有账号进行登录 b) 输入账号口令，点击登录，抓取登录数据包进行分析
预期结果	a) 至少具备两种身份鉴别方式 b) 被抓取的数据包中，身份鉴别信息被加密，无法被识别
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.1.5
安全要求	a) 根据组织的安全要求，可根据现实场景（如网络环境、系统环境、设备类型等）制定登录策略，进行登录控制。（可选） b) 宜对相同终端上的重复登录行为进行识别和管控。（可选）
预置条件	无
测试方法	a) 检查是否支持制定登录策略； b) 检查是否对重复登录行为进行识别和管控。
预期结果	a) 具备登录策略制定； b) 对重复登录行为可实现识别管控。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

9.2 权限

编号	6.2-a
安全要求	在访问业务资源前，应先对用户成功地进行身份鉴别，并能够根据用户相应的访问权限返回业务数据。
预置条件	系统在未登录状态下
测试方法	a) 检查各类角色登录后，角色权限是否与定义权限一致。 b) 用户登出后，不应因浏览器缓存等因素仍能打开链接。
预期结果	a) 角色权限应与定义权限一致 b) 文件或图片链接无法被访问或打开
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.2-b
安全要求	可采用已登录终端设备扫码授权的方式进行授权登陆。（可选）

预置条件	在终端设备上已登录
测试方法	a) 使用已登录状态终端扫码授权未登录系统。
预期结果	a) 未登录系统成功登录
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.2-c
安全要求	应对已停用账号的访问权限进行控制。
预置条件	用户在正常登录状态
测试方法	a) 在管理后台选择一个账户，将其停用或删除
预期结果	a) 在账户被停用后，此账户将无法访问系统内的各项资源
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

9.3 错误锁定

编号	6.3-a
安全要求	应针对在规定时间内多次身份鉴别失败的用户进行锁定，在规定时间内进行解锁。
预置条件	系统已有账号，且管理后台开启此项功能，获取重试失败错误次数配置
测试方法	a) 选用一个已有账号，多次输入错误的口令（或其他鉴别方式） b) 在规定时间内再次尝试
预期结果	a) 多次输入错误口令后，账号应被锁定 b) 在规定时间内再次尝试，可解除锁定
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.3-b
安全要求	可对在规定时间内多次修改口令或找回口令的用户进行锁定，在规定时间内进行解锁。 (可选)
预置条件	系统已有账号，且管理后台开启此项功能，获取重试失败错误次数配置
测试方法	a) 选用一个已有账号进行口令找回操作，多次重复操作 b) 在规定时间内再次尝试
预期结果	a) 多次输入错误口令后，账号应被锁定 b) 在规定时间内再次尝试，可解除锁定
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.3-c
安全要求	在登录错误信息返回时，应采用模糊提示。
预置条件	无
测试方法	a) 选用一个已有账号，输入错误的口令（或其他鉴别方式）

预期结果	a) 获得模糊的错误提示用语（未明确是账号错误和口令错误）
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

9.4 账号口令

编号	6.4-a
安全要求	应对口令复杂度进行控制，包括口令长度、字符组成等。应避免使用含有账号信息的口令及常见口令。
预置条件	无
测试方法	a) 新注册账号，设置初始口令 b) 输入 111111、123456、888888 等常见口令作为账号的初始口令
预期结果	a) 新设计的口令，应符合管理后台设置的口令复杂度要求 b) 输入常见口令后，系统应给以提示，并要求设置符合复杂度要求的口令
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.4-b
安全要求	可具有口令找回或口令重置的能力，并具备验证机制。（可选）
预置条件	无
测试方法	a) 选用一个已有账号，进行口令找回操作
预期结果	a) 具有此能力； b) 找回或重置过程中，具备验证机制
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.4-c
安全要求	可对口令变更周期进行控制。（可选）
预置条件	无
测试方法	a) 选用一个已有账号，且口令多日未修改，超出变更周期，并尝试登录；
预期结果	a) 系统需提示用户需要修改口令
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.4-d
安全要求	不应默认保存用户上次的账号及口令。
预置条件	无
测试方法	a) 打开系统登陆界面，查看输入框内容
预期结果	a) 默认没有保存用户上次的账号及口令
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	6.4-e
安全要求	修改身份鉴别方式时，可验证原有身份鉴别方式。（可选）
预置条件	处于系统登录状态
测试方法	a) 选用一个已有账号，并成功登录； b) 在系统中进行修改口令操作；
预期结果	a) 修改口令过程中需验证原有身份鉴别方式
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10 应用层安全测试方法

10.1 通讯录管理

编号	7.1
安全要求	a) 应支持组织架构可见性设置；支持隐藏敏感字段。 b) 宜支持手机号安全查看审计，宜支持查看数量达到上限的提醒策略。（可选）
预置条件	系统部署完成，通讯录创建完成
测试方法	管理员登录控制台， a) 设置用户 A、部门 B 对所有人隐藏 b) 设置用户 C 限制查看外部门 c) 开启手机号安全查看选项
预期结果	a) 其它用户登录，用户 A、部门 B 不在通讯录显示 b) 用户 C 登录，只看查看到本部门的通讯录 c) 通讯录查看个人信息，手机号显示“点击查看”。查看人数超过一定数量，会进行提示。管理员在后台可以对手机号查看动作进行审计。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.2 授权管理

编号	7.2
安全要求	宜支持分级制授权管理，指定组织节点分配分组管理员，实现集中管理、分层授权。（可选）
预置条件	系统部署完成，通讯录创建完成
测试方法	管理员登录控制台， a) 创建分级管理员 b) 设置该分级管理员的管理范围 c) 分配该分级管理员的通讯录管理权限
预期结果	a) 使用该分级管理员登录控制台 b) 对于管理范围内的组织架构具有管理权限 b) 对于非管理范围内的组织架构不具有权限
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.3 聊天申请

编号	7.3
安全要求	可支持对聊天权限的灵活控制，在触达不可见成员（如非好友非同事等）的场景下，可设置聊天申请权限。（可选）
预置条件	系统部署完成，通讯录创建完成
测试方法	管理员登录控制台， a) 设置用户 A、部门 B，其它人需要申请通过才能开始聊天 b) 设置用户 B 为白名单，不受聊天申请规则限制
预期结果	a) 用户 C 登录客户端，向用户 A、部门 B 的人员发起聊天。系统提示发送聊天申请 b) 被申请人同意聊天申请后，用户 C 可以聊天。 c) 用户 B 登录客户端，向用户 A、部门 B 的人员发起聊天，可正常聊天。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.4 敏感信息过滤

编号	7.4
安全要求	宜支持敏感信息过滤，管理员可在后台设置需要过滤掉的敏感信息。导入成功后，系统自动通过敏感信息匹配而进行信息拦截。（可选）
预置条件	系统部署完成
测试方法	管理员登录控制台， a) 添加消息敏感词，如“暴力” b) 用户登录客户端，发送一条消息如“足球暴力” c) 发送一个如包含“足球暴力”的文本文件
预期结果	a) 系统提示“消息涉及敏感信息”，消息发送失败 b) 系统提示“消息涉及敏感信息”，文件发送失败。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.5 背景水印

编号	7.5
安全要求	a) 应支持聊天显示水印。 b) 可支持管理员配置在“聊天”、“通讯录”、“头像”、“邮件”、“网页”、“文件”等不同位置单独设置开、关水印功能。（可选） c) 水印显示的内容宜支持定制，如“姓名”、“手机号后四位”、“日期”、“邮箱”或者自定义字样。（可选）
预置条件	系统部署完成
测试方法	管理员登录控制台， a) 设置客户端水印。设置在“聊天”、“通讯录”、“头像”、“邮件”、“网页”、“文件”等显示水印。 b) 设置水印内容为“姓名”、“手机号后四位”、“日期”、“邮箱”或者自定义字样。
预期结果	a) 用户登录客户端，“聊天”、“通讯录”、“头像”、“邮件”、“网页”、“文件”等界面显示水印，水印内容为当前用户的“姓名”和“手机号后四位”、“日期”、“邮箱”或者自定义字样。

判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合
------	---------------------------

10.6 消息撤回

编号	7.6
安全要求	a) 应支持用户个人撤回指定时间内的消息。 b) 可支持群管理员远程撤回。（可选）
预置条件	系统部署完成
测试方法	a) 用户登录客户端，发送一条消息。 b) 一定时间内，可以撤回该消息。 c) 管理员后台查询消息 ID，通过工具撤回该消息
预期结果	a) 用户可在一定时间内撤回消息成功。 b) 管理员可以撤回用户发出的消息。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.7 消息防控

编号	7.7
安全要求	宜支持管理员在后台进行移动端安全管理设置，实现如消息防复制、防转发、防保存、防分享、防截屏、防录屏等功能。（可选）
预置条件	系统部署完成
测试方法	管理员登录控制台，启用如下设置 1) 禁用成员在客户端“接收”和“拍摄”的图片或视频保存到手机相册。 2) 禁用聊天记录分享到微信或外部即时通讯工具 3) 仅在当前App内复制粘贴 4) 禁用文件在其它应用打开或保存到手机 5) 禁用网页分享（包含复制链接，分享到微信和朋友圈，在外部浏览器打开等入口） 6) 禁用通过邮件发送 6) 用户A给用户B发送一条文本消息、发送一张图片、发送一个Word文件、一个网页链接
预期结果	a) 用户 B 登录客户端， b) 长按收到图片，不显示保存菜单，无法保存图片到本地相册。 b) 多选消息，点击转发，不显示转发菜单，无法将消息转发到微信。 c) 复制收到的文本消息，切换到短信 App，粘贴文本消息。文本消息没有被复制。 d) 选中收到的文件，长按，不显示第三方打开菜单，无法将文件发给第三方应用。 e) 网页链接仅支持内部打开，不显示外部打开菜单，无法使用系统浏览器打开网页。 f) 打开文件，不显示邮件发送菜单，无法将文件通过邮件附件发送。
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.8 消息推送

编号	7.8
安全要求	移动消息推送应支持不显示发信人和内容摘要。
预置条件	系统部署完成
测试方法	a) 管理员登录控制台，启用“通知不显示消息详情” b) 用户 B 客户端处于离线状态 c) 用户 A 给用户 B 发送一条消息。
预期结果	a) 用户 B 收到一条消息提示 b) 消息提示不显示发送者姓名，不显示消息内容
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.9 群管理

编号	7.9
安全要求	a) 应支持群成员邀请确认。 b) 可支持群禁言，包括全部禁言、部分禁言等。（可选） c) 应支持群管理的权限设置。
预置条件	系统部署完成
测试方法	a) 用户 A 创建一个群，将多个用户加入群聊天 b) 用户 A 设置启用“群聊邀请确认”。用户 B 邀请其它用户入群。 c) 用户 A 设置群内全部禁言，仅允许群主发言。 d) 用户 A 设置部分成员禁言，设置用户 B 禁言。 e) 用户 A 将设置用户 B 为群管理员，用户 B 进行群管理操作 f) 用户 A 设置群主转让为用户 B。
预期结果	a) 用户 B 邀请其它用户入群，系统提示群已设置群聊邀请确认，提示向群主说明理由 b) 用户 A 收到群邀请提示，可查看邀请详情信息，并确认邀请。用户即可加入群聊。 c) 全员禁言后，用户 B 群内发送消息，系统提示已开启群禁言，消息无法发送。 d) 用户 B 被禁言后，群内发送消息，系统提示已被群禁言，消息无法发送。 e) 用户 B 被设置为群管理员后，可以进行群管理操作。 f) 用户 B 被转让为群主后，可以以群主身份进行群管理相关操作
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.10 音视频管控

编号	7.10
安全要求	a) 应支持对音视频业务数据进行加密保护 b) 可支持对音视频业务的接入人员进行管控。（可选） c) 可支持音视频业务的禁止录音、禁止录屏、禁止截图等。（可选）
预置条件	无
测试方法	a) 检查音视频业务数据是否加密； b) 是否具备能力对音视频业务接入人员进行管控； c) 是否支持音视频业务的禁止录音、禁止录屏、禁止截图等。
预期结果	a) 音视频业务数据进行加密保护； b) 可对接入人员进行有效管控 c) 具备能力对录音、录屏、截图等进行阻断。

判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合
------	---------------------------

10.11 动态密钥

编号	7.11
安全要求	可支持动态密钥认证，实现不联网或应用加固被破解场景下的敏感数据防泄漏。（可选）
预置条件	终端处于不联网状态
测试方法	a) 使用终端本地密钥对消息和文件进行解密
预期结果	a) 无法通过终端本地密钥直接对消息和本地文件进行解密从而获取明文数据
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

10.12 检测与扫描接口

编号	7.12
安全要求	可支持病毒检测、敏感信息扫描接口。（可选）
预置条件	系统部署完成，第三方病毒检测、敏感信息扫描系统部署完成
测试方法	a) 管理员开启检测与扫描功能
预期结果	a) 发送一个正常文件，成功。 b) 发送一个存疑的问题，系统发出可能存在病毒等提示。 c) 发送一个包含病毒的文件，系统发出文件中存在病毒等提示。 d) 发送一个敏感信息存疑的文件，系统发出文件中可能存在敏感信息等提示。 e) 发送一个敏感信息文件，系统发出文件中存在敏感信息等提示。”
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

11 通信安全测试方法

11.1 通信协议

编号	8.1
安全要求	a) 传输层协议应采用TCP或UDP协议。 b) 应用层协议应采用可扩展通讯和表示协议（XMPP）、即时消息和表示协议（IMPP）、即时消息协议（PRIM）、SIP即时消息和表示扩展协议（SIMPLE）、超文本传输安全协议（Https）等其中一种协议。 c) 可支持私有协议，具备一定可读性和扩展性。（可选）
预置条件	--
测试方法	a) 客户端模拟发送/接收消息等场景； b) 抓取客户端与服务端之间的连接数据包；

预期结果	a) 传输层协议为TCP或UDP协议; b) 应用层协议为私有协议、可扩展通讯和表示协议 (XMPP)、即时消息和表示协议 (IMPP)、即时消息协议 (PRIM)、SIP即时消息和表示扩展协议 (SIMPLE)、超文本传输安全协议 (Https) 的一种或多种;
判定准则	上述预期结果均满足判定为符合, 其他情况判定为不符合

11.2 接入安全

编号	8.2.1
安全要求	a) 遵循最小权限原则, 系统具备核心数据应做到仅开放当前接入用户可访问的范围。 核心数据包括: 消息、联系人数据、文件等企业用户私密数据。 b) 系统的业务功能应做到按需开放, 接入用户仅可以使用当前拥有权限的功能范围。
预置条件	--
测试方法	a) 在系统端对用户限制业务功能及相应数据访问权限;
预期结果	a) 客户端上登录该用户时, 所展示的数据及功能入口, 符合系统端设置;
判定准则	上述预期结果均满足判定为符合, 其他情况判定为不符合

编号	8.2.2
安全要求	宜具备对接入用户的审计能力。(可选)
预置条件	--
测试方法	a) 在客户端上登录用户, 登录系统端查看审计内容;
预期结果	a) 在系统端可以查看到登录记录, 审计内容包括: 接入设备名称、接入用户、重要用户行为、接入时间等;
判定准则	上述预期结果均满足判定为符合, 其他情况判定为不符合

11.3 传输安全

编号	8.3.1
安全要求	1、数据传输过程中应支持TLS 1.2 (RFC 5246, 2008) 及以上安全协议。 2、数据传输过程中可支持国密算法。(可选)
预置条件	--
测试方法	a) 抓取客户端连接服务端的数据包; b) 在管理端/客户端开启国密配置, 重新抓取客户端连接服务端的数据包;
预期结果	a) 客户端功能使用正常。同时验证数据包的协议为 TLS 1.2, 验证其通道加密套件为 TLS 1.2 标准加密算法;

	b) 客户端功能使用正常。验证数据包中 TLS 协商的加密算法为国密算法套件 (SM2/SM3/SM4)
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	8.3.1
安全要求	公有云即时通信软件可支持端到端加密。（可选）
预置条件	公有云即时通讯系统下两个软件终端a/b互相发送消息
测试方法	a) a 发送一条信息给 b； b) 抓包 a 发送的报文，通过服务端的公钥对密文进行解析； c) 最终透传到终端 b，正常展示消息内容
预期结果	a) 终端 a 发送出去的内容为密文，无法通过服务端公钥进行解析 b) 终端 b 接收到信息在本地通过本地会话密钥解析显示
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合

编号	8.3.1
安全要求	密钥应具备更新机制且支持多版本管理，确保不影响业务持续性。
预置条件	—
测试方法	a) 登录管理端查看是否具有密钥更新机制（自动更新或手动更新）并可进行相关设置； b) 登录管理端查看是否支持多版本管理功能；
预期结果	a) 具备密钥更新机制，管理端支持密钥更新配置、管理等相关功能。 b) 旧密钥已加密存储至历史库中；
判定准则	上述预期结果均满足判定为符合，其他情况判定为不符合