## A.1用例模型浏览

## **A.1.1简略描述**

| **维度** | **内容** |
| --- | --- |
| **谁来使用本用例模型** | 网民（平台用户）、安全与合规管理员、聊天运营管理员、数字支付运营管理员、在线网银系统（外部）与（可选）商户系统 |
| **人们要求系统做什么** | 即时沟通（文本/语音/视频）与安全、可追溯的数字支付；在异常情况下能够审计、合规处置与账务纠偏 |
| **到底是什么** | 一个为用户提供安全便捷的社交沟通与支付结算服务的综合性数字平台，构建沟通与交易的闭环体验 |
| **本系统的目的** | 让用户在可信条件下完成一对一通信与单笔支付；同时让管理员能进行风控、合规与运营维护 |
| **本系统并不会** | 暴露底层UI细节或硬件驱动流程；替代银行清结算职能；绕过监管要求 |
| **我们的产品** | 7×24 可用；接口与外部网银系统安全互联；所有关键操作可审计、可追溯 |

## **A.1.2参与者类别**

图1给出了WeChat中的所有参与者，下面小节给出了这些参与者的简略描述。

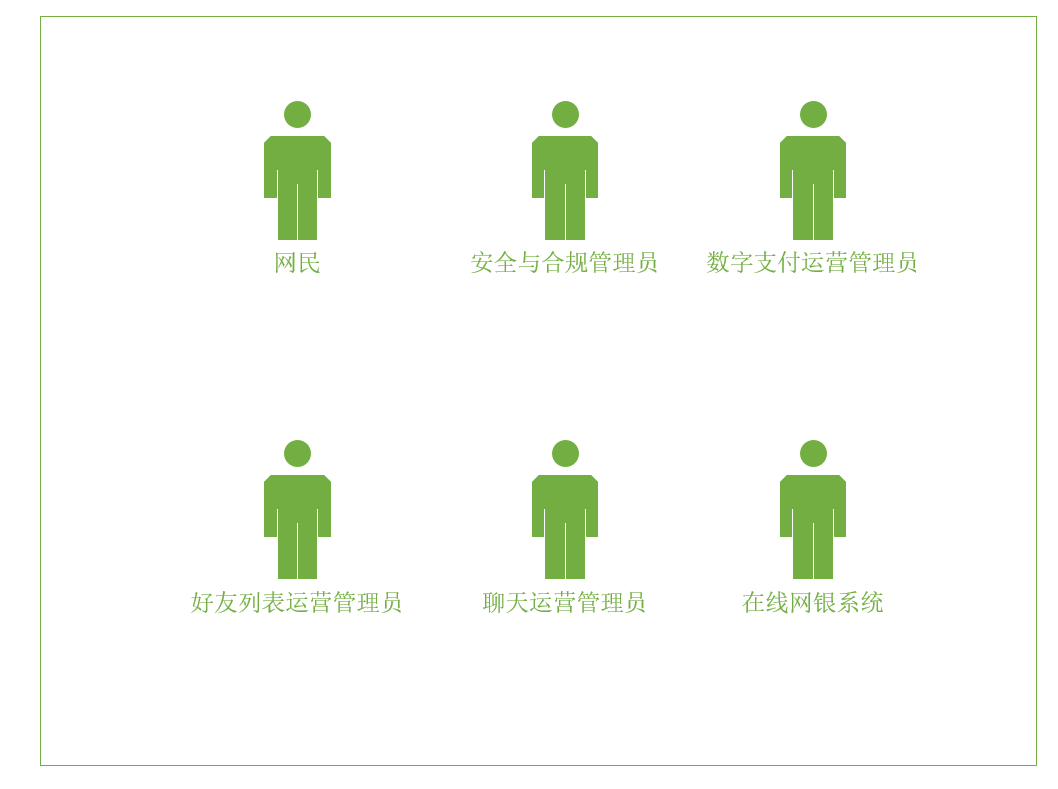


图1 WeChat中的参与者

**1.网民（Customer/User）**

在客户端发起与接收通信；在支付场景中提交支付请求、接收结果与回执。主叫/被叫均视为此参与者。

**2.安全与合规管理员（Security & Compliance Admin）**

关注敏感内容、违规与可疑交易；查看告警、处置冻结/解冻、生成合规报告。

**3.聊天运营管理员（Chat Ops Admin）**

监控通信可用性与质量告警；查询会话留痕；处理用户举报并回访。

**4.数字支付运营管理员（Payment Ops Admin）**

关注支付通道健康、对账差异与补偿；配置限额与风控策略；查看运营报表。

**5.在线网银系统（Bank System）**

为本系统提供扣款/转账授权、返回同步/异步结果、输出清单用于对账。

## **A.1.3用例类别**

**1.主要用例**

图2给出了WeChat用况模型中的主要用例。下面小节则给出这些用例的简略描述。

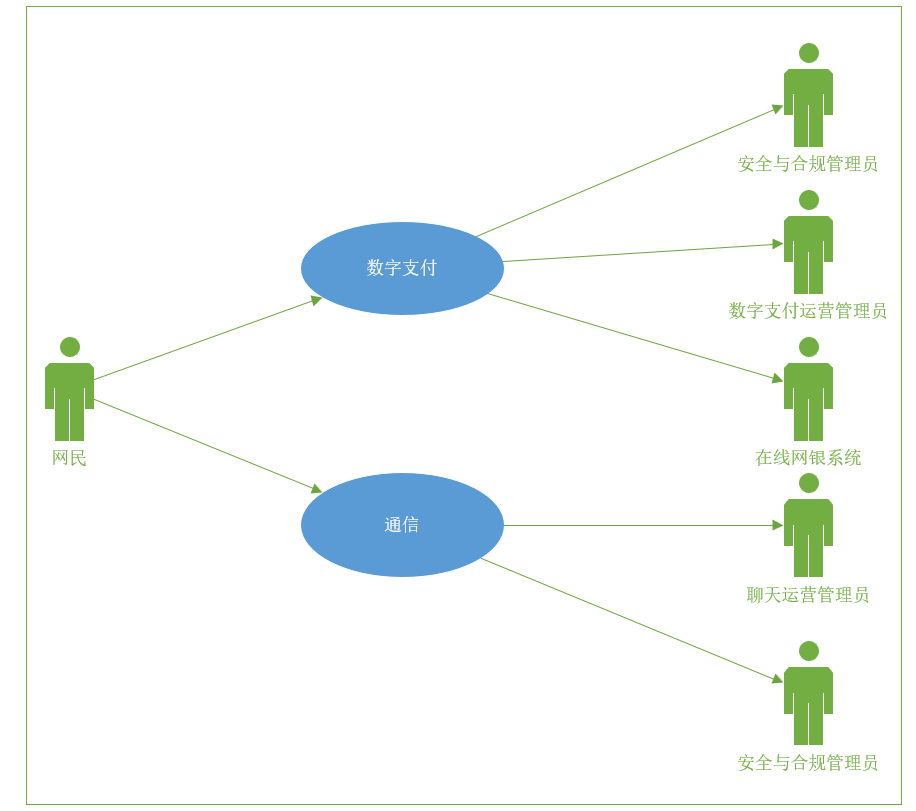
****

图2 WeChat主要用例

通信：网民与网民之间建立一对一会话（文本/语音/视频），支持敏感词过滤、举报与会话留痕。

数字支付：网民对单笔订单完成支付；系统执行风控与授权、结果入账、异步对账/补偿。

**2.补充用例**

合规处置：对内容违规/可疑交易进行记录、上报与冻结/解冻（由管理员驱动）。

运营监控与对账：监控通道与质量、生成对账与补偿报告、留痕审计。

## A.2用例描述——通信(UC-1)

## **1. 简略描述**

该用例描述了网民如何通过系统与另一网民建立一对一实时通信，支持文本消息、语音通话和视频通话三种通信模式，并确保通信过程的安全性和合规性。

## **2. 用例图**

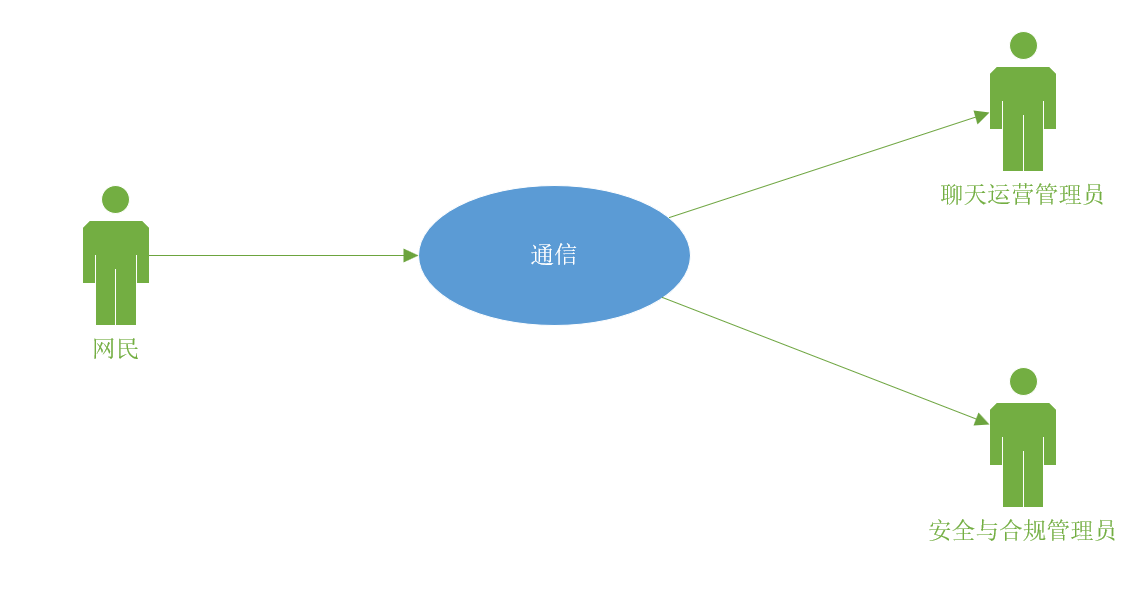


图3 通信用况的用况图

## **3. 前置条件**

1.通信双方网民均已成功登录系统；

2.通信双方网民互为好友或存在于可通信列表中；

3.系统网络连接正常且可用；

4.网民设备的相关硬件（麦克风、摄像头等）可用且已授权；

## **4. 基本流**

{建立连接}

1. 用例开始时，参与者网民从联系人列表中选择目标网民。

2. 参与者网民选择通信模式（文本、语音或视频）。

3. 系统向目标网民发送会话邀请。

4. 系统等待目标网民响应，最多30秒。

5. 如果目标网民接受邀请，系统建立通信信道并通知双方连接成功。

{进行通信}

6. 根据通信模式执行相应子流：

- 如果通信模式为文本：Perform S1 处理文本消息交换

- 如果通信模式为语音：Perform S2 维护语音通信

- 如果通信模式为视频：Perform S3 维护视频通信

{结束通信}

7. 当任一网民选择结束通信时，系统执行子流 S4 结束通信会话。

8. 用例终止。

## **5. 备选流**

**A1处理邀请被拒绝**

**At {建立连接} if 目标网民拒绝邀请**

1.系统通知参与者网民"对方已拒绝您的通信邀请"；

2.用例终止；

**A2处理邀请超时**

**At {建立连接} if 目标网民在30秒内未响应邀请**

1.系统通知参与者网民"对方无应答"；

2.用例终止；

**A3处理目标网民正忙**

**At {建立连接} if 检测到目标网民正在其他通信会话中**

1.系统通知参与者网民"对方正忙，请稍后再试"；

2.用例终止；

**A4处理网络质量下降**

**At {进行通信} when 系统检测到网络质量严重下降**

1.系统自动降低音频码率以保证通话连贯性；

2.系统自动降低视频分辨率或建议网民暂停视频；

3.系统在界面显示"网络连接质量不佳"提示；

4.通信流程从检测到问题的地方继续；

**A5处理通信中断**

**At {进行通信} when 通信连接意外中断**

1.系统自动尝试重新建立连接；

2.如果30秒内无法重新连接，系统记录通信中断事件；

3.系统通知双方网民"通信连接已中断"；

4.执行子流 S4 结束通信会话；

5.用例终止；

**A6处理内容违规**

**At {进行通信} when 系统检测到多次敏感内容**

1.系统记录违规事件并生成合规报告；

2.系统向安全与合规管理员发送通知；

3.系统可临时限制该网民的通信功能；

4.通信流程从检测到违规的地方继续；

**A7处理网民举报**

**At {进行通信} when 任一网民举报对方**

1.系统记录举报信息并保存通信记录；

2.系统向聊天运营管理员发送举报通知；

3.通信流程从举报发生的地方继续；

**A8 处理网民无响应**

**At {进行通信} when 网民在60秒内无操作**

1.系统发出提示音提醒网民；

2.如果继续无响应，系统显示"会话即将超时结束"警告；

3.如果120秒内仍无响应，执行子流 S4 结束通信会话；

4.用例终止；

**6. 子流（Named Subflows）**

**S1处理文本消息交换**

1. 系统建立文本消息传输通道。

2. 当参与者网民发送文本消息时：

a. 系统接收消息并执行实时敏感词过滤。

b. 如果消息包含敏感词，系统用"\*\*\*"替换敏感词并记录审核日志。

c. 系统将处理后的消息实时投递给目标网民。

d. 系统在双方界面显示消息。

3. 持续执行直到收到结束通信信号。

4. Resume at the next step.

**S2：维护语音通信**

1. 系统建立高质量语音数据通道；

2. 系统开始捕获、编码、传输双方的语音数据；

3. 系统实时监控网络质量，动态调整音频参数；

4. 系统处理回声消除和背景降噪；

5. 如果检测到网络质量下降，系统自动调整码率优先保证通话连贯性；

6. 持续执行直到通信结束；

7. 返回到调用点；

**S3：维护视频通信**

1. 系统建立结合视频和语音的数据通道；

2. 系统开始捕获、编码、传输双方的视频和语音数据；

3. 系统实时监控网络和性能，动态调整视频分辨率；

4. 系统支持前后摄像头切换功能；

5. 系统支持视频暂停功能（暂停后保持语音通信）；

6. 如果检测到网络质量下降，系统优先保证语音质量；

7. 持续执行直到通信结束；

8. 返回到调用点；

**S4：结束通信会话**

1. 系统断开通信信道；

2. 系统记录会话日志，包括：

开始时间和结束时间；

通信参与者；

通信模式；

会话时长；

3. 系统生成合规审核记录；

4. 系统释放相关资源；

5. 返回到调用点；

## **7. 后置条件**

1.通信会话已被完整记录，包括开始时间、结束时间、通信模式和参与者信息；

2.必要的安全与合规审核记录已生成（如涉及敏感内容或用户举报）；

3.系统资源已被正确释放；

4.用户通信状态已更新；

## **8. 特殊需求**

性能要求:

文本消息投递延迟：小于1秒；

语音通话延迟：低于400毫秒；

视频通话延迟：低于500毫秒；

系统可用性：99.5%以上；

安全要求:

所有通信内容必须进行实时敏感词过滤；

语音和视频通信必须采用加密传输；

用户隐私数据必须得到保护；

合规要求:

通信记录必须保存至少90天；

敏感内容触发必须实时记录并报告；

用户举报必须及时处理并记录；

## A.4用例描述——数字支付(UC-2)

## **1. 简略描述**

网民通过系统完成一笔单笔订单的数字支付；系统完成请求接收、风控与合规校验、向在线网银系统发起授权、结果入账与通知，并保证可追溯与对账一致性。

## **2. 用例图**

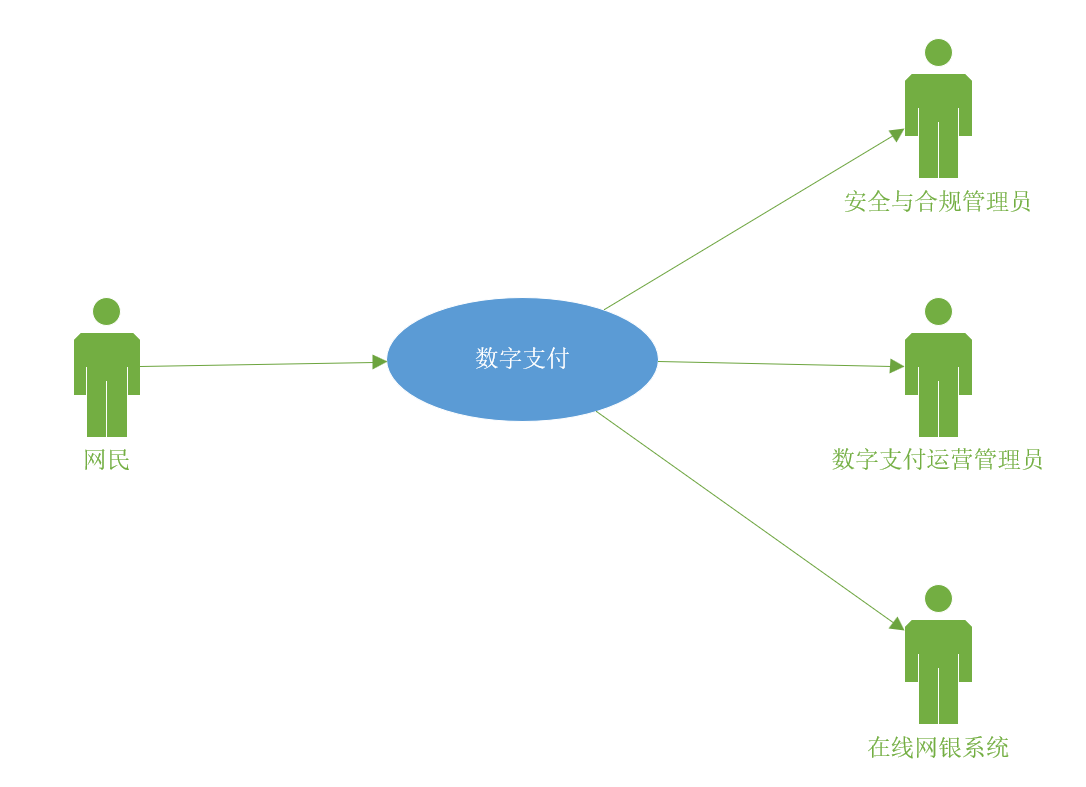


图4 数字支付用况的用况图

**3. 前置条件**

 1.网民已登录且支付账户处于**可用**状态（通过必要的 KYC/实名校验）；

 2.目标订单存在、未支付、未过期，金额与收款方信息完整有效；

 3.支付方式（银行卡/账户余额等）已绑定且允许本次交易限额；

 4.系统与在线网银系统网络连通、签名/证书有效。

**4. 基本流**

{接收支付请求}

1.系统接收网民提交的支付请求（订单号、金额、收款标识、支付方式等）。

2.系统创建支付交易并置状态为“待授权”，记录审计上下文（设备、IP、时间）。

{校验与风控}

3.系统执行 S1 风控与合规校验。若通过，继续；否则转入备选流 A1/A7。

{发起银行授权}

4.系统根据支付方式选择路由，调用 S2 银行授权处理，向在线网银系统发起扣款/转账授权请求。

5.系统等待授权结果，最长 60 秒。

{结果处理}

6.系统接收授权结果：

-如果返回"成功"：系统执行 S3 结果入账与通知

-如果返回"处理中"：系统标记交易为"待确认"，执行 S4 异常补偿与对账

7.系统向网民展示支付结果。

8.用例终止。

**5. 备选流**

**A1 风控拒绝**

**At {校验与风控} if 命中高风险/黑名单/限额：**

1.系统将交易置“拒绝”，保存拒绝原因与证据；

2.通知网民“风险拦截，交易未受理”；

3.发送告警给安全与合规管理员；

4.用例终止。

**A2 余额不足 / 账户受限**

**At {发起银行授权} when 网银返回资金不足或账户限制：**

1.记录失败码并将交易置“失败”；

2.通知网民失败原因；

3.用例终止。

**A3 银行系统超时**

**At {发起银行授权} when 60 秒内未获结果：**

1.系统按退避策略重试至上限；

2.若仍超时，置交易为“待确认”，记录对账待跟踪条目；

3.进入 S4 异常补偿与对账；

4.返回{结果处理}继续。

**A4二要素/3-DS 挑战**

**At{发起银行授权} when 网银要求额外认证：**

1.系统转发挑战需求并收集认证结果；

2.若认证通过，返回{发起银行授权}继续授权；

3.若认证失败或超时，置“失败”，用例终止。

**A5 用户取消**

**At {接收支付请求} when 网民在授权前撤销：**

1.系统将交易置“已取消”并解除幂等锁；

2.用例终止。

**A6 重复支付防重**

**At {接收支付请求} if 检测到相同订单号与幂等键已成功：**

1.系统直接返回已成功结果与原回执；

2.用例终止。

**A7 合规疑似（需人工复核）**

**At {校验与风控} when 命中可疑模式（反洗钱/套现）：**

1.置交易为“冻结待核查”，生成合规工单；

2.通知安全与合规管理员；

3.用例暂止，待人工处置后按结论走 S3 或置失败。

**A8 回调丢失/账务不一致**

**At {结果处理} when 异步对账发现银行已成功而本地未落账：**

1.触发 S4 异常补偿与对账进行补记账与通知；

2.记录“补偿成功/失败”；

3.返回{结果处理}结束。

**A9 网银系统不可用**

**At{发起银行授权} when 通道故障：**

1.切换备用通道或置交易“系统繁忙”；

2.通知运营管理员；

3.用例终止或进入 A3 流程。

**A10 网民长时间无操作**

**At {接收支付请求} when 15 分钟未完成授权：**

1.系统关闭交易为“超时关闭”；

2.用例终止。

**6. 子流（Named Subflows）**

**S1 风控与合规校验**

1. 系统验证订单信息的完整性和有效性，包括订单号、金额、收款方标识。
2. 系统检查交易金额是否在用户单日及单笔限额范围内。
3. 系统验证交易频率是否符合安全规则，防止高频异常交易。
4. 系统检查设备指纹、地理位置信息和IP地址是否存在异常模式。
5. 系统查询用户账户是否在黑名单或高风险名单中。
6. 系统执行反洗钱规则检查，识别可疑交易模式。
7. 如果发现中等风险行为，系统要求用户进行额外身份验证。
8. 如果发现高风险行为，系统触发人工复核流程并生成合规工单。
9. 系统记录所有风控检查的审计轨迹和决策依据。
10. Resume at the next step.

**S2 银行授权处理**

1. 系统根据支付方式选择对应的银行通道和接口协议。
2. 系统组装银行授权请求报文，包括交易金额、商户信息、用户标识。
3. 系统对请求报文进行数字签名和加密处理。
4. 系统与在线网银系统建立安全加密通道。
5. 系统发送授权请求到银行系统并启动响应计时器。
6. 系统接收银行系统的同步响应或受理回执。
7. 如果银行要求额外认证，系统转发挑战需求并收集用户认证结果。
8. 系统解析银行响应，提取授权码、交易状态和错误信息。
9. 系统记录完整的银行交互报文摘要和时序信息。
10. 系统更新交易状态为"已授权"或根据响应设置相应状态。
11. Resume at the next step.

**S3 结果入账与通知**

1. 系统依据银行授权结果更新交易状态：
2. 如果授权成功：更新为"支付成功"
3. 如果授权失败：更新为"支付失败"并记录失败原因
4. 系统执行原子记账操作，确保资金账户余额准确更新。
5. 系统生成唯一的电子回执号和交易凭证。
6. 系统记录完整的账务分录，包括借方、贷方账户和金额。
7. 系统向参与者网民发送支付结果通知，包括成功/失败状态和交易详情。
8. 系统向商户系统发送支付成功通知（如适用）。
9. 如果交易涉及风险或合规事件，系统向安全与合规管理员发送告警通知。
10. 系统持久化所有交易日志、审计信息和操作痕迹。
11. 系统更新相关业务系统的订单状态为"已支付"。
12. Resume at the next step.

**S4 异常补偿与对账**

1. 系统生成对账任务，设置对账时间窗口和重试策略。
2. 系统从在线网银系统拉取指定时间段的交易清单。
3. 系统将本地交易记录与银行交易清单进行逐笔比对：
4. 识别"银行成功而本地未入账"的交易
5. 识别"银行失败而本地误入账"的交易
6. 识别金额不一致的交易记录
7. 对于比对发现的差异交易，系统执行相应的补偿操作：
8. 如果是"银行成功而本地未入账"：执行补记账操作并补发通知
9. 如果是"银行失败而本地误入账"：执行冲正操作并通知相关方
10. 如果是金额不一致：暂停交易并生成人工处理工单
11. 系统更新交易状态为最终确定状态。
12. 系统生成对账报告，包括总交易数、成功数、差异数和处理结果。
13. 系统将对账结果通知数字支付运营管理员。
14. 系统归档完整的对账记录和补偿操作日志。
15. Resume at the next step.

**7. 后置条件（成功保证）**

1.交易状态为“成功”或“待确认/冻结/关闭”等终结性或可追踪状态；

2.账务分录、回执、审计日志与对账条目完整可追溯；

3.若触发合规事件，相关报告/工单已生成并通知到位；

4.与在线网银系统的交互记录可核验。

**8. 特殊需求**

**性能要求：**

-支付交易处理时间：小于3秒；

-系统并发处理能力：支持每秒1000笔交易；

-系统可用性：99.9%以上；

-支付结果通知延迟：小于1秒；

**安全要求：**

-所有支付数据传输必须采用加密传输；

-支付密码输入必须使用安全键盘；

-大额交易必须进行多重身份验证；

-用户支付信息必须安全存储；

**合规要求：**

-支付交易记录必须保存至少5年；

-单笔交易超过一定金额必须报告监管部门；

-可疑交易必须实时记录并报告；

-用户隐私数据必须得到保护；

**审计要求：**

-所有支付操作必须生成审计日志；

-系统管理员操作必须记录操作痕迹；

-支付状态变更必须记录变更历史；

## A.4补充术语表术语

| **术语** | **说明** | **补充信息** |
| --- | --- | --- |
| **网民** | 使用本系统进行通信与支付的最终用户。 | 与“主叫网民/目标网民”为**同一参与者类型**在会话中的不同角色； |
| **主叫网民** | 在通信用例中**发起**会话邀请的网民（会话内的瞬时角色）。 | 仅在会话期间有效；与“网民”同类型；常用字段：caller\_id、邀请时间、会话ID。 |
| **目标网民** | 被主叫选定并接收邀请的一方。 | 与主叫同为“网民”类型的**对等体**；常用字段：callee\_id、可达/忙闲状态。 |
| **聊天运营管理员** | 负责通信可用性与质量监控、处理用户举报、查看会话留痕。 | 不处理支付账务与通道对账；需要处置与查询权限。 |
| **安全与合规管理员** | 监控敏感内容与可疑交易，执行合规审核、冻结/解冻、报送。 | 生成/审阅合规报告；不负责运营SLA与日常运行指标。 |
| **数字支付运营管理员** | 负责支付通道健康、限额/策略配置、对账与补偿处置。 | 关注差异交易处理与运营报表；不处理聊天内容或举报。 |
| **在线网银系统** | 银行侧授权/清算与对账清单提供者，对接支付请求并返回结果。 | 外部系统，通过受信安全通道（证书/签名）连接； |