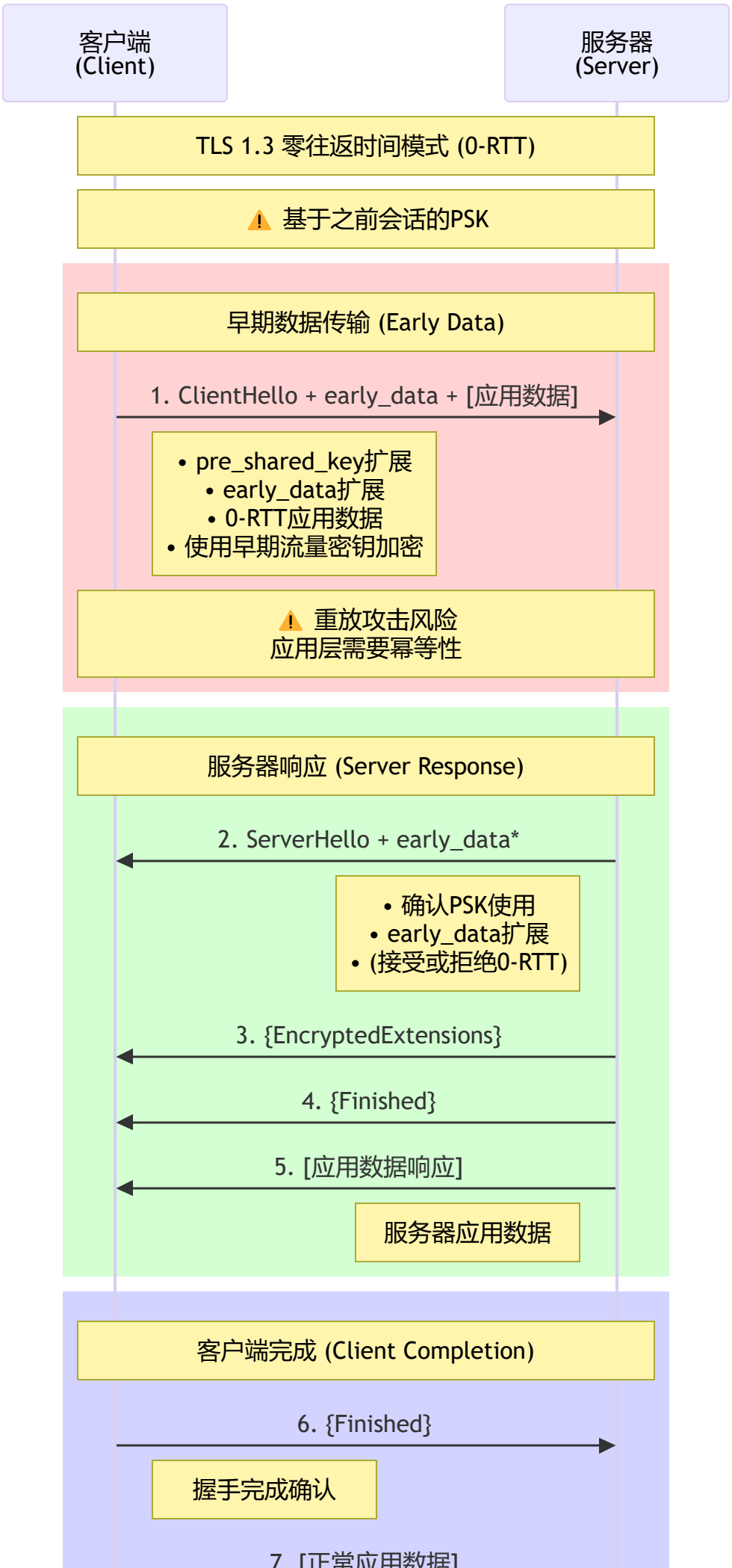
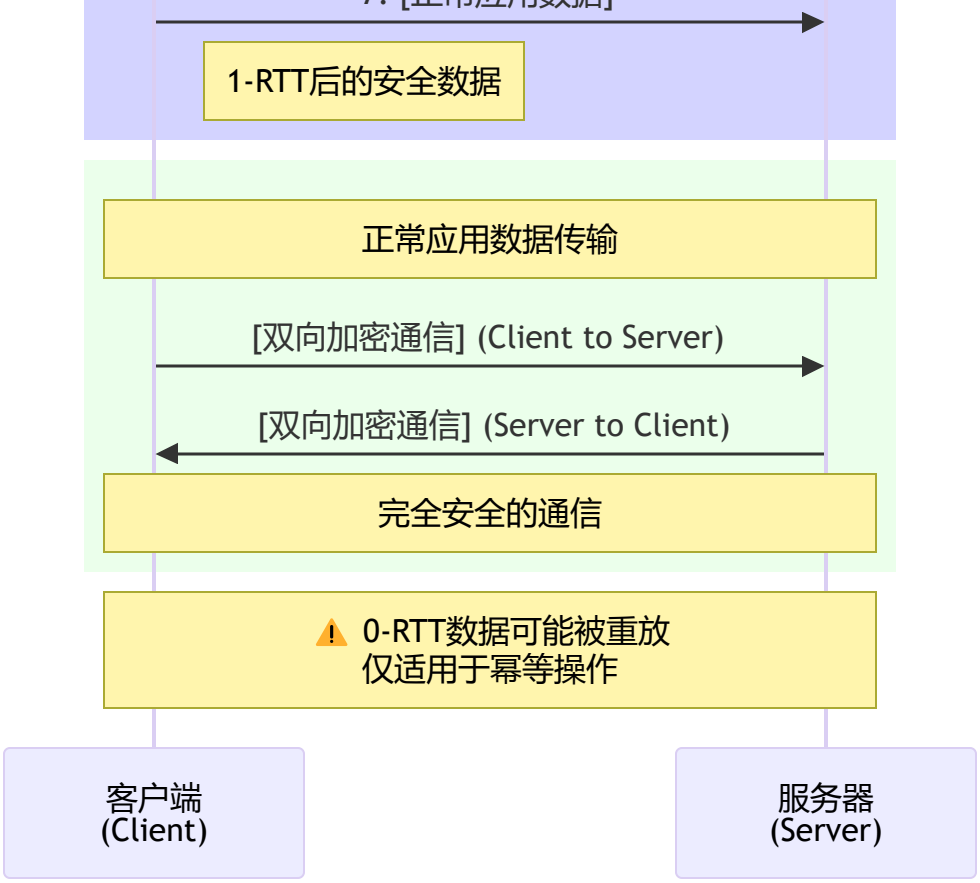

客户端
(Client)
服务器
(Server)
TLS 1.3 零往返时间模式 (0-RTT)
⚠ 基于之前会话的PSK
早期数据传输 (Early Data)
1. ClientHello + early_data + [应用数据]
• pre_shared_key扩展
• early_data扩展
• 0-RTT应用数据
• 使用早期流量密钥加密
⚠ 重放攻击风险
应用层需要幂等性
服务器响应 (Server Response)
2. ServerHello + early_data*
• 确认PSK使用
• early_data扩展
• (接受或拒绝0-RTT)
3. {EncryptedExtensions}
4. {Finished}
5. [应用数据响应]
服务器应用数据
客户端完成 (Client Completion)
6. {Finished}
握手完成确认
7. [正常应用数据]


7. [正常应用数据]
1-RTT后的安全数据
正常应用数据传输
[双向加密通信] (Client to Server)
[双向加密通信] (Server to Client)
完全安全的通信
⚠ 0-RTT数据可能被重放
仅适用于幂等操作
客户端
(Client)
服务器
(Server)