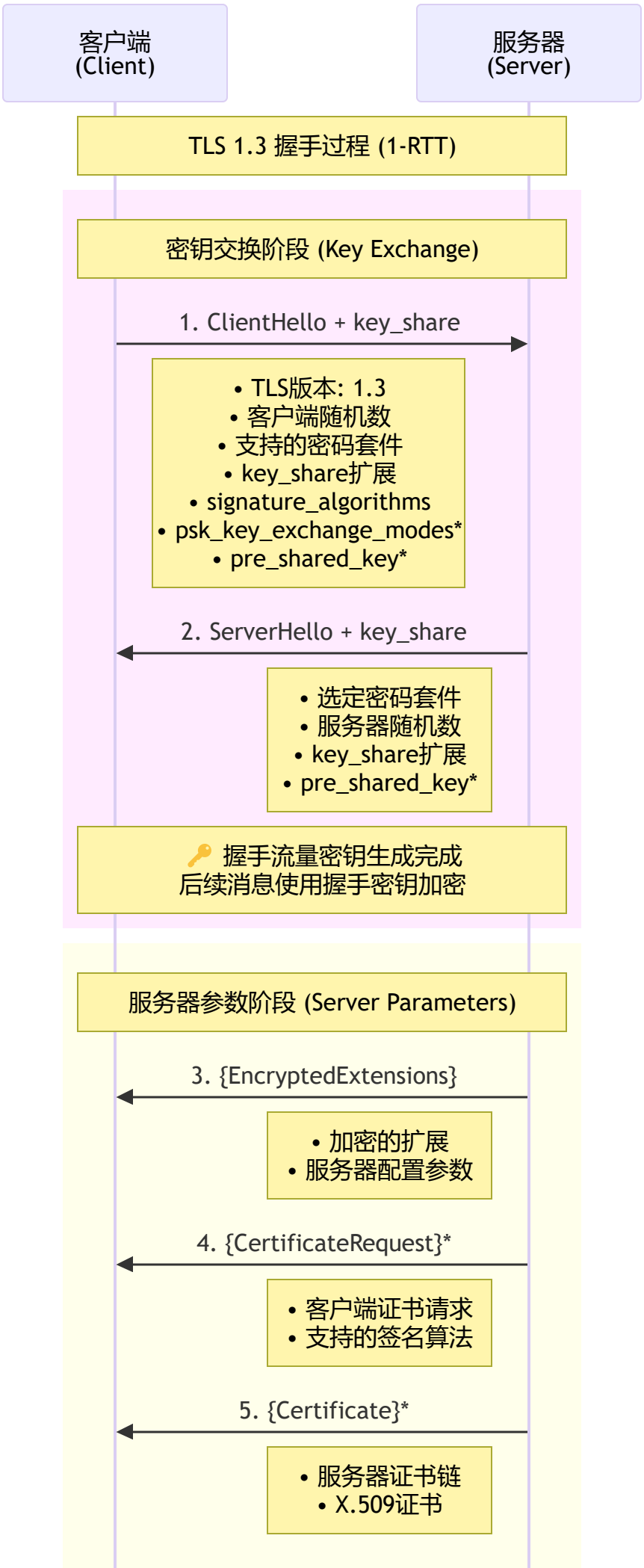
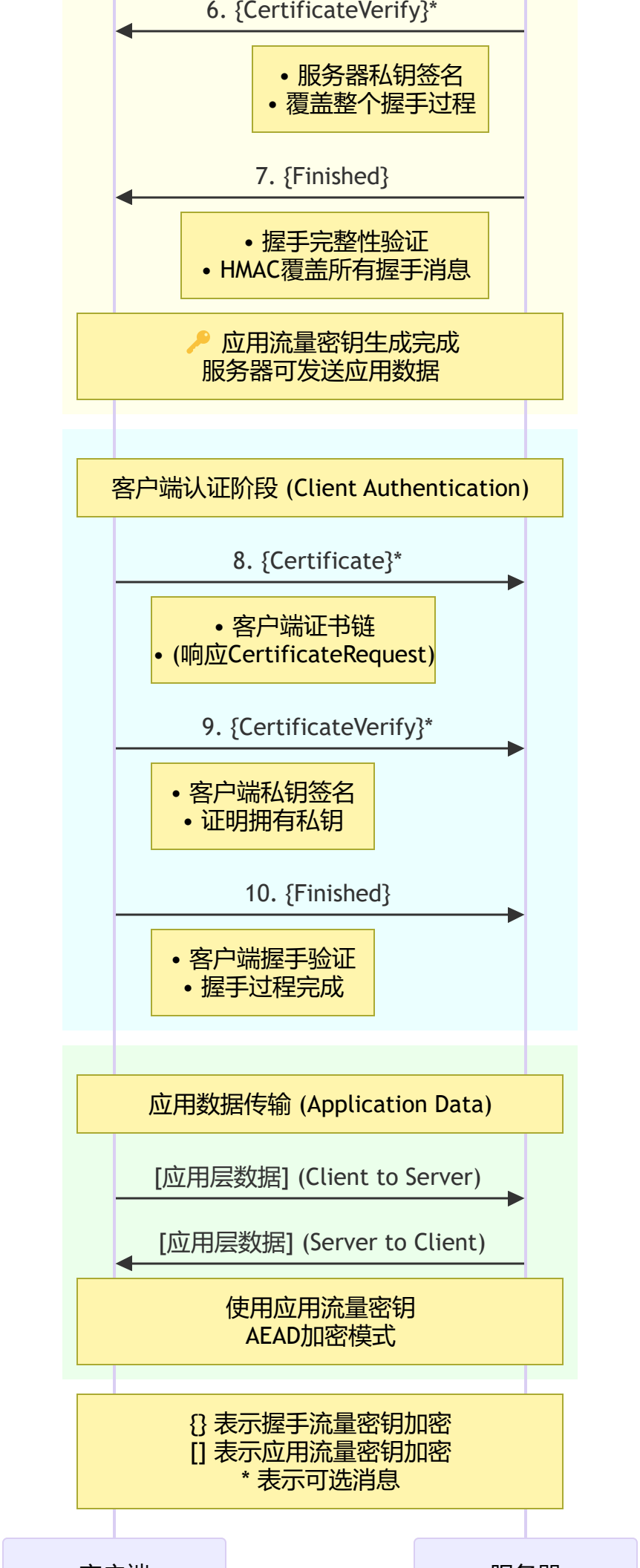

客户端
(Client)
服务器
(Server)
TLS 1.3 握手过程 (1-RTT)
密钥交换阶段 (Key Exchange)
1. ClientHello + key_share
• TLS版本: 1.3
• 客户端随机数
• 支持的密码套件
• key_share扩展
• signature_algorithms
• psk_key_exchange_modes*
• pre_shared_key*
2. ServerHello + key_share
• 选定密码套件
• 服务器随机数
• key_share扩展
• pre_shared_key*
🔑 握手流量密钥生成完成
后续消息使用握手密钥加密
服务器参数阶段 (Server Parameters)
3. {EncryptedExtensions}
• 加密的扩展
• 服务器配置参数
4. {CertificateRequest}*
• 客户端证书请求
• 支持的签名算法
5. {Certificate}*
• 服务器证书链
• X.509证书


6. {CertificateVerify}*
• 服务器私钥签名
• 覆盖整个握手过程
7. {Finished}
• 握手完整性验证
• HMAC覆盖所有握手消息
🔑 应用流量密钥生成完成
服务器可发送应用数据
客户端认证阶段 (Client Authentication)
8. {Certificate}*
• 客户端证书链
• (响应CertificateRequest)
9. {CertificateVerify}*
• 客户端私钥签名
• 证明拥有私钥
10. {Finished}
• 客户端握手验证
• 握手过程完成
应用数据传输 (Application Data)
[应用层数据] (Client to Server)
[应用层数据] (Server to Client)
使用应用流量密钥
AEAD加密模式
{} 表示握手流量密钥加密
[] 表示应用流量密钥加密
* 表示可选消息


客户端
(Client)
服务器
(Server)