Atitit info secr tech vpn https 端到端加密

**端到端加密**（英語：End-to-end encryption，縮寫：E2EE），是一種只有参与通讯的用户可以读取信息的通信系统

**不留记录即时通讯**（Off-the-Record Messaging，縮寫為OTR）是一種[安全協議](https://zh.wikipedia.org/wiki/%E5%AE%89%E5%85%A8%E5%8D%94%E8%AD%B0" \o "安全協議)，為[即時通訊](https://zh.wikipedia.org/wiki/%E5%8D%B3%E6%99%82%E9%80%9A%E8%A8%8A" \o "即時通訊)提供加密保護。OTR使用128bit長度的[高级加密标准](https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86" \o "高级加密标准)（AES）[對稱密鑰加密](https://zh.wikipedia.org/wiki/%E5%B0%8D%E7%A8%B1%E5%AF%86%E9%91%B0%E5%8A%A0%E5%AF%86" \o "對稱密鑰加密)保護，1536bits的[迪菲－赫尔曼密钥交换](https://zh.wikipedia.org/wiki/%E8%BF%AA%E8%8F%B2%EF%BC%8D%E8%B5%AB%E5%B0%94%E6%9B%BC%E5%AF%86%E9%92%A5%E4%BA%A4%E6%8D%A2" \o "迪菲－赫尔曼密钥交换)（D-H）與[SHA-1](https://zh.wikipedia.org/wiki/SHA-1" \o "SHA-1)函數。在加密與驗證機制之外，OTR同時提供[前向保密](https://zh.wikipedia.org/wiki/%E5%89%8D%E5%90%91%E4%BF%9D%E5%AF%86" \o "前向保密)（Forward secrecy）功能。

另一种选项是使用**传输中加密**，发送方先将加密消息并传输至服务器，服务器加密、重新加密并传送至接收方，最后接收方再解密。传输中加密可以在消息传输过程中保护信息安全，但是服务器可以看见消息内容，根据服务器拥有者的不同可信程度，有时这可能会存在隐患。

# 端到端加密通信软件？

​

知乎十年新知答主

电子邮件不就是么？

有的人居然说电子邮件不够实时？你们没有用过电子邮件客户端吗？尤其是集团的像 outlook exchange 那样的企业版。

当年根本没有即时通讯，绝大多数功能是完全用邮件实现的：

* 双人对话：双人单发邮件
* 群聊：群发邮件，回复的时候点回复全部。
* 群：预定义邮件列表，部分可以存在outlook里边，比如研发部，运营部，客服部，往这个列表发邮件就是群发了，然后回复的时候回复全部就相当于群消息。（当然你可以随时回复邮件中的某一个人，相当于私聊）
* 语音：邮件可以直接发语音，发图片，发文件，只不过当年的电脑没有普及摄像头所以好像很少有视频功能，不过技术上应该也没有什么难度的。
* 投票，通知：这些都是可以在企业平台内实现的功能，无论是 exchange 体系还是 lotus note 体系都可以

没加“即时”两个字就可以有。比如非著名邮件客户端thunderbird的插件enigmail就支持基于gpg的加密邮件。很多其他邮件客户端也支持加密邮件，当然，前提是你用pgp/gpg。

如果需要加“即时”两个字的话，考虑到腾讯系的软件使用非官方扩展会被封号，除非你能够忍受手动复制粘贴加解密，不然就只能自己实现了。

如果只是自用，那么其实你不需要e2ee，因为你不需要不信任自己的服务器，这样的话其实TLS就足够了。