```
-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.0
u2R4d+/jKmn8Bc5+hgDsqAewsDfrGdszX68liKm5F6Gc4sDfcXyt
RfdS10juHgbcfDssWe7/K=lKhnMikLo0+1/BvcX4t==Ujk9PbcD4
Thdf2awQfgHbnmKlok8iy6gThlp
-----END PGP MESSAGE
```

图 8-23 一个秘密 PGP 报文

PGP 也提供了一种公钥认证机制，但是这种机制与更为传统的 CA 差异很大。PGP 公钥由一个可信 Web 验证。当 Alice 相信一个密钥/用户名对确实匹配时，她自己就可以验证这一密钥/用户名对。此外，PGP 允许 Alice 为她所信任的用户鉴别更多密钥提供担保。一些 PGP 用户通过保持密钥签署方（key-signing party）互相签署对方的密钥。用户实际走到一起，交换公钥，并用自己的私钥对对方的公钥签名来互相验证密钥。

8.6 使 TCP 连接安全：SSL

在前一节中，我们看到对一个特定的应用（即电子邮件），密码技术是怎样提供机密性、数据完整性和端点鉴别的。在这一节中，我们在协议栈中向下一层，考察密码技术如何用安全性服务加强 TCP，该安全性服务包括机密性、数据完整性和端点鉴别。TCP 的这种强化版本通常被称为**安全套接字层**（Secure Socket Layer，SSL）。SSL 版本 3 的一个稍加修改的版本被称为**运输层安全性**（Transport Layer Security，TLS），已经由 IETF 标准化［RFC 4346］。

SSL 最初由 Netscape 设计，而使 TCP 安全隐含的基本思想先于 Netscape 的工作（例如，参见［Woo 1994］）。由于 SSL 的崭露头角，它已经得到了广泛部署。SSL 得到了所有流行 Web 浏览器和 Web 服务器的支持，并基本上被用于所有因特网商业站点（包括 Amazon、eBay、Yahoo!、MSN 等等）。每年经 SSL 花费了数百亿美元。事实上，如果你使用信用卡通过因特网购买任何东西的话，在你的浏览器和服务器之间的通信几乎一定使用了 SSL。（当你使用浏览器时，若 URL 以 https：开始而不是以 http 开始，就能认定正在使用 SSL。）

为了理解 SSL 的需求，我们浏览一下某典型的因特网商业的场景。Bob 在 Web 上冲浪，到达了 Alice 公司的站点，这个站点正在出售香水。Alice 公司站点显示了一个表格，假定 Bob 可以在该表格中输入香水的类型和所希望的数量、他的地址和他的支付卡号等信息。Bob 输入这些信息，点击“提交”，就期待收到（通过普通邮政邮件）所购买的香水；他也期待着在他的下一次支付卡报表中收到对所购物品的支付信息。所有这一切听起来不错，但是如果不采取安全措施，Bob 也许会有一些意外。

- 如果没有使用机密性（加密），一个入侵者可能截取 Bob 的订单并得到他的支付卡信息。这个入侵者则可以用 Bob 的费用来购买商品。
- 如果没有使用完整性，入侵者可能修改 Bob 的订单，让他购买比希望瓶数多 10 倍的香水。
- 最后，如果没有使用服务器鉴别，这个显示 Alice 公司著名徽标的服务器实际上是由 Trudy 维护的一个站点，Trudy 正在假冒 Alice 公司。当 Trudy 收到 Bob 的订单后，可能拿了 Bob 的钱一走了之。或者 Trudy 可能充当一名身份窃贼，收集 Bob 的名字、地址和信用卡号。

SSL 通过采用机密性、数据完整性、服务器鉴别和客户鉴别来强化 TCP，就可以解决