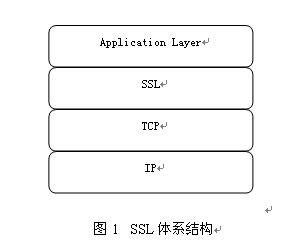
https 实际在应用层与tcp之间增加ssl校验层，如图



主要通过证书、非对称加密、对称加密来进行校验

证书：是为了客户端识别是否为某证书服务器

非对称加密：校验是否可确立连接主要，对确立连接阶段的网络传输提供加密（握手协议）

对称加密：确立安全连接后对数据的加密服务

补：对称加密：双方拿着相同的钥匙

非对称加密：由提供数据一方持有私钥，使用数据一方使用公钥加密

Ssl认证过程：

一次认证过程包括次tcp连接 证书本身包含一对公私钥、ssl需要的一份公私钥

* 首先客户端通过https协议请求服务器，服务器返回证书、公钥、ssl、加密算法等相关信息
* 客户端校验返回的证书合法性，如果合法通过公钥对当前生成的对称密钥进行加密传给服务器，服务器接受到使用私钥解密后进行响应，确认客户端可使用对称加密密码------握手完成
* 客户端与服务端通讯，通过对称加密进行数据加密