图解HTTP(8) 确认访问用户身份的认证1

1 通常要核对的信息

- 密码：只有本人才会知道的字符串信息。
- 动态令牌：仅限本人持有的设备内显示的一次性密码。
- 数字证书：仅限本人（终端）持有的信息。
- 生物认证：指纹和虹膜等本人的生理信息。
- IC 卡等：仅限本人持有的信息。

2 HTTP/1.1 使用的认证方式
BASIC（基本认证，明着传送 通过base64加密的账号密码。guest : guest ==> 对应的base64编码进行传送）、
DIGEST认证（摘要认证，感觉是 BASIC的”加强版“，质询码【随机生成】）
SSL客户端认证【安装证书，费用、成本较高，稍微少用】
FormBase认证【基于表单认证，上面那几个不也是？？！】

3 DIGEST【BASIC加强版，也是一样使用的 质询 / 响应 的方式】
质询 / 响应： 2方【客户端】请求了一个需要认证的资源， 然后1方【服务端】先发 认证要求【含质询码】过去； 2方 使用 1方 发送过来的质询码计算生成响应吗；最后将响应码 返回给对方进行认证。

四 SSL客户端认证【需要借助 HTTPS】
1 从使用 账号密码 的这类 认证方式来讲，只要二者的内容正确，即可认证是本人所为【不合理，存在盗号风险】
SSL客户端认证是 借由HTTPS 的客户端证书 完成认证的方式.
服务器可以确认访问是否来自 自己登陆的客户端？？ 【自己登陆的客户端？？！】。

五 基于表单认证【不是HTTP 中所定义的】！！
基于表单认证的方法不是在HTTP协议中定义的。
客户端向 服务器上 的 web应用 发送登录信息 ， 然后服务器上的web应用 根据 登录信息 去验证结果。

补： 防止 XSS ， Cookie处 设置 httponly属性【这样只有 HTTP‘响应’才能读取 cookie， JS脚本不能读取 cookie了】！！

完