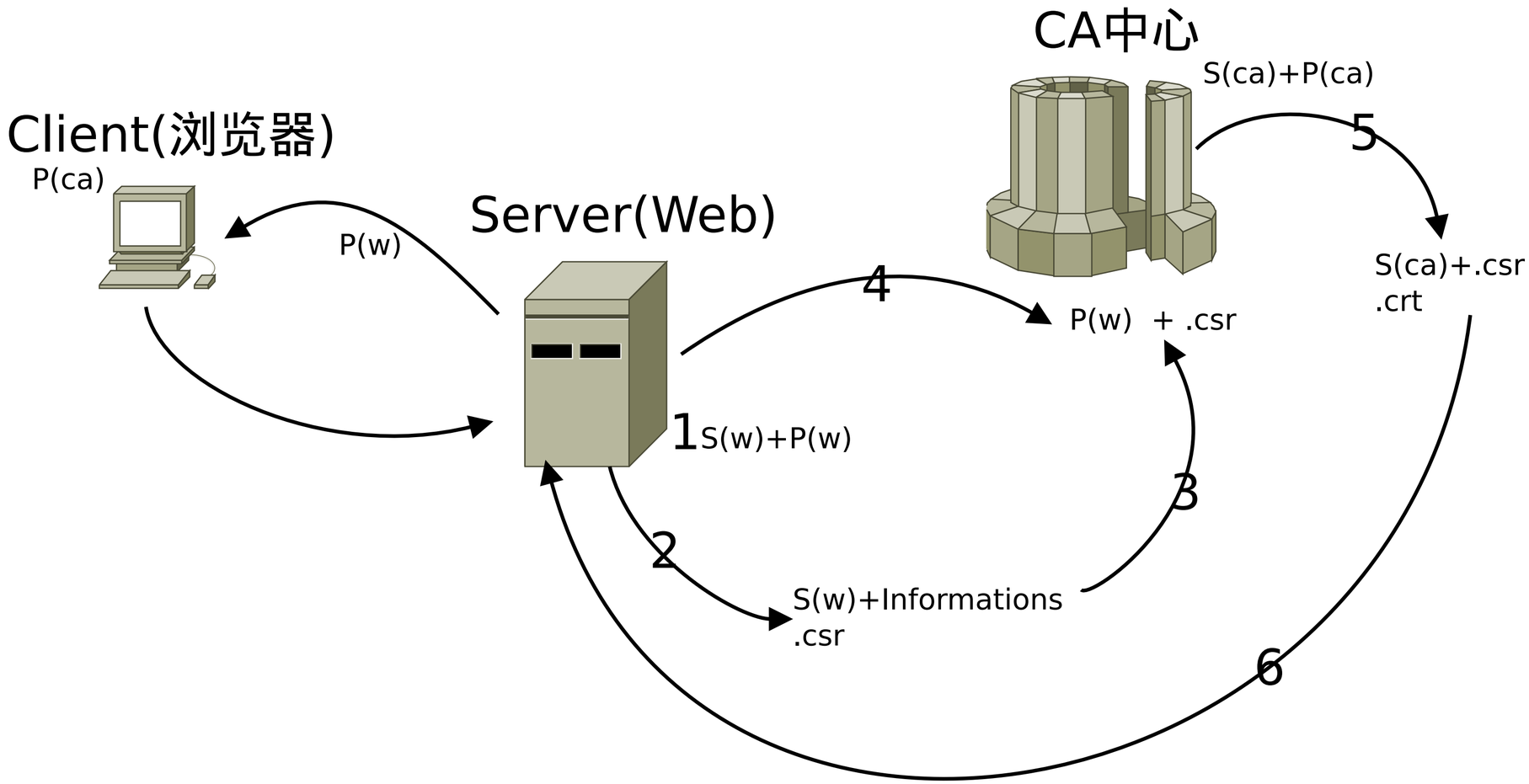

1、服务器生成一对非对称密钥。公钥P(w)+私钥S(w)。
2、服务器利用自己的私钥加密自己的主机信息【S(w)+Informations】，生成.csr文件。
3、服务器将.csr文件用各种途径，比如邮寄等，提交给CA中心。
4、CA中心得到.csr文件，通过网络得到服务器的公钥P(w)解密得到.csr中的信息，
并经过审核得到的信息正确。
5、CA中心利用自己的私钥S(ca)加密.csr得到.crt文件返还给服务器。【S(ca)+.csr=.crt】
6、服务器得到.crt文件后在机器的机器上安装.crt文件。
7、客户端的浏览器本身自带各CA中心的P(ca)。加上它浏览服务器就可以得到P(w)。