●对应于个人公用密匙的公用密匙字段560（4），ID代码560（5）（在该实例中，可以是公用密匙字段560（3）的散列），以及

●提供错误校验功能的校验和字段560（6）。

在该实例中，数字凭证504（1）被认证机构500利用该认证机构的公用密匙－私用密匙密码系统的的私用密匙，如RSA或EI Gamal加密。认证机构500的相应的公用密匙可以公开（如将它发布在一些公开的WWW站点上或其它广泛分布的环境中），或者予以保密，不向受保护的处理环境154的外部披露。在其中任意一种情况下，将数字凭证504（1）成功地解密，揭示其原始的明文信息，这提供了高度的保障，即该数字凭证的确是认证机构500颁发的（假设认证机构的私用密匙尚未泄密）。

期满字段560（3）之所以有用，是因为忽略撤销目录校验的人至少有一点相信，即如果凭证必须周期性地更新，那么它就是好的。期满字段560（3）通过确保凭证不会永远持续有效，提供了另外一层保护－使认证机构 500 可以使用不同的密匙对来提供认证处理的完整性和可信度。变更认证机构500的密匙减少了对手破译某个密匙的动机，因为受密匙保护的信息量是有限的，欺诈性地使用泄密的密匙将只有有限的有效时间。而且，（目前）数学上尚未预见到的进展可能会使某些加密算法无用武之地，因为它们依赖的是（目前）理论上可以难以处理的计算。如果启用新的算法重新颁发凭证，那么内建的变更认证机构500密匙的机制，就会将这种破解密匙的影响限制在一段时间内（或者，可以使用根据不同算法生成的多个不对称的密匙对，给密匙作标记并使之生效，从而消除这个风险，其代价是额外的加密时间）。

图51B、51C和51D示出了另外一个含有不同种类信息（如在凭证504（5）情况下为专业凭证字段560（7），在凭证504（3）情况下为地址字段信息 560（8），以及在学生证 504（2）情况下为学生凭证信息504（9））的数字凭证的实例。这些凭证504（2）、504（3）、504（5）通过公用ID字段560（5）与身份证504（1）结合在一起，通常要求同时出示身份证和独立的凭证。

图 51E 示出了认证机构所颁发的示例性的数字凭证怎样能够－与可信的数据库一起－成为其它认证机构批准其它凭证的依据。认证机构500A能够，例如，使用户身份生效并创建图51A所示的身份证504(1)。