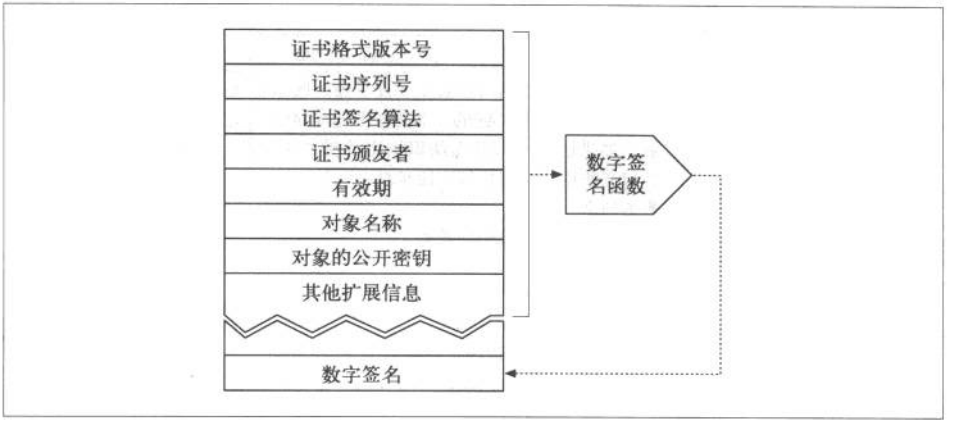

图 14-11　典型的数字签名格式

14.6.2　X.509 v3证书

不幸的是，数字证书没有单一的全球标准。就像不是所有印刷版 ID 卡都在同样的位置包含了同样的信息一样，数字证书也有很多略有不同的形式。 不过好消息就是现在使用的大多数证书都以一种标准格式——X.509 v3，来存储它们的信息。X.509 v3 证书提供了一种标准的方式，将证书信息规范至一些可解析字段中。不同类型的证书有不同的字段值，但大部分都遵循 X.509 v3 结构。表 14-2 介绍了 X.509 证书中的字段信息。

表14-2　X.509证书字段

字　段	描　述
版本	这个证书的 X.509 证书版本号。现在使用的通常都是版本 3
序列号	证书颁发机构（CA）生成的唯一整数。CA 生成的每个证书都要有一个唯一的序列号
签名算法 ID	签名所使用的加密算法。例如，“用 RSA 加密的 MD2 摘要”
证书颁发者	发布并签署这个证书的组织名称，以 X.500 格式表示
有效期	此证书何时有效，由一个起始日期和一个结束日期来表示
对象名称	证书中描述的实体，比如一个人或一个组织。对象名称是以 X.500 格式表示的
对象的公开密钥信息	证书对象的公开密钥，公开密钥使用的算法，以及所有附加参数
发布者唯一的 ID（可选）	可选的证书发布者唯一标识符，这样就可以重用相同的发布者名称
对象唯一的 ID（可选）	可选的证书对象唯一标识符，这样就可以重用相同的对象名称了

320