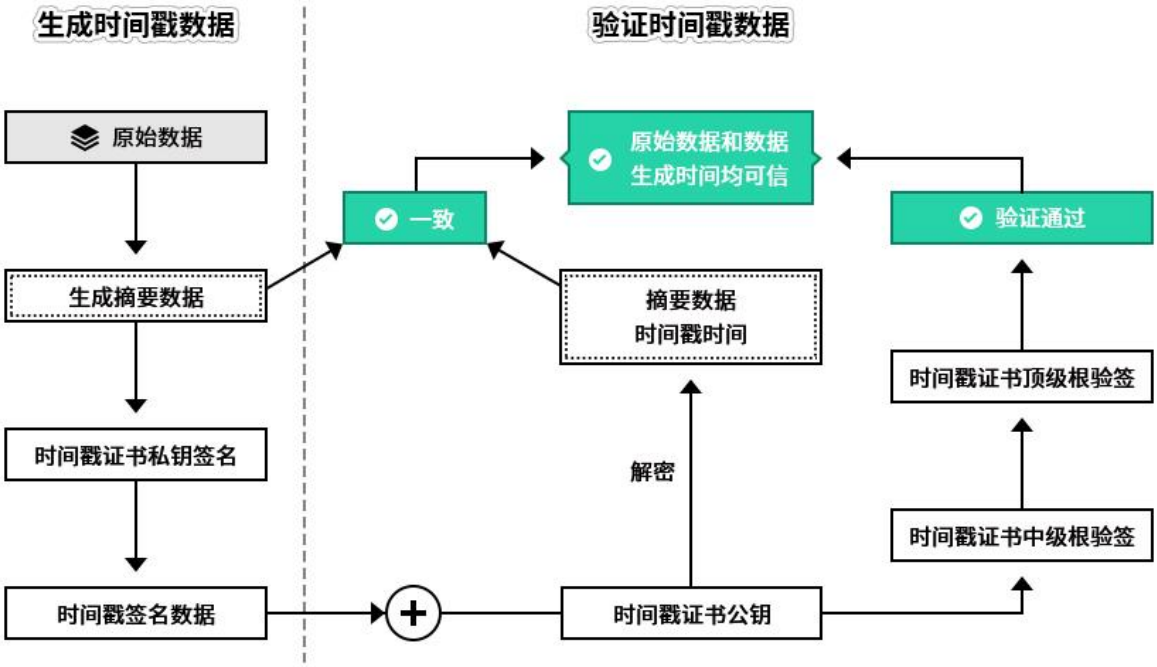
时间戳，大数据时代必配字段

(2021 年 4 月 27 日)

什么是时间戳？时间戳就是使用数字签名技术产生的签名数据，签名的对象包括了原始数据、签名参数和签名时间等信息。时间戳系统用来产生和管理时间戳数据，使用时间戳证书对签名对象进行数字签名产生时间戳数据，以证明原始数据在签名时间之前已经存在，并且之后不能修改，这样就能保证当时记录的事件时间和数据都是原始数据，是没有被修改的数据。

现在是大数据时代，各种智能网联汽车的行车数据都会上传到云端，如何事后证明行车数据是原始数据而不是厂商自己事后“制造”的数据？唯一可行的方案是在数据产生时不仅记录数据本身，还需要把记录的数据提交到第三方时间戳服务获取时间戳签名数据，并把这个时间戳数据单独作为一个字段同原始数据一起存放云端数据库中。这样，事后如果需要这些数据，可以调出原始数据和时间戳签名数据，相关方就可以通过验证时间戳数据来判断当时的原始数据是否真实可信。

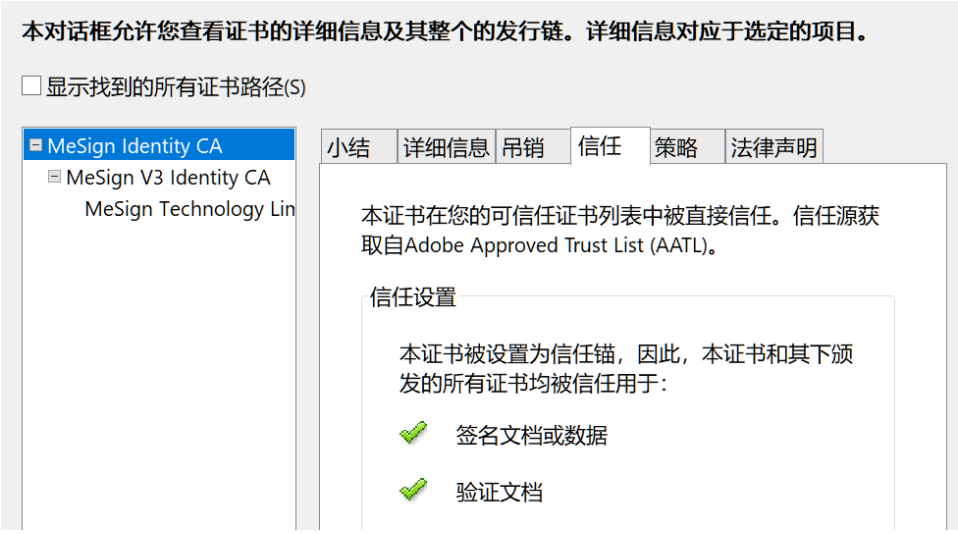
时间戳数据生成和验证原理如下图所示:



先对原始数据生成摘要(HASH)数据，再调用第三方时间戳服务，时间戳服务系统使用时间戳证书私钥签名摘要数据生成时间戳签名数据。需要验证原始数据是否可信时，只需使用时间戳证书公钥解密时间戳签名数据，计算出原始数据的摘要数据和可信的时间戳时间，就可以对

比数据库中的原始数据的摘要数据是否一致，一致则说明原始数据没有被篡改。还要用签发时间戳证书的中级根验证时间戳证书是否可信，再用顶级根证书验证中级根证书是否可信，如果通过验证，则说明的确是用的第三方时间戳服务。再加上摘要数据验证一致，就可以证明原始数据是可信的原始数据。至于当时数据库的记录时间是否可信，应该以时间戳时间为准，数据库记录时间仅供参考。

其实，不仅仅是行车数据，各种视频监控数据、医院的诊断和检查数据、公检法数据、电子政务办事审批数据等等都有可能需要日后审计和查验，如何证明这些数据生成时间可信和未被事后篡改，都需要调用可信的第三方时间戳服务来证明。密信时间戳证书经过严格的 WebTrust 审计并已经预置 Adobe 全球信任，密信时间戳服务由 360 安全云提供安全运维服务，值得信赖。下图为 Adobe 阅读器显示的 Adobe 信任密信根证书信息。



如果需要同时证明数据生产者的身份可信，则还需要同时用数据生产者的签名证书数字签名数据，验证签名数据时也是按照上述同样方法验证签名者身份可信，证明此数据的确是某单位生产的和确信数据没有被篡改，同时通过验证时间戳签名数据证明数据生产时间可信。也就是说，如果只用时间戳签名服务，则只能证明数据未篡改和证明当时提交时间戳签名的时间可信；而如果同时用用户证书签名，则还能证明数据的确是某人或某单位生产，这个数字签名可以用于判断数据所属权，适合于需要证明数据产权的应用场景。

为此，笔者呼呼 CIO 们应该立刻行动起来，尽快安排更新管理信息系统的数据库结构，增加一个时间戳签名数据字段，并选购密信时间戳服务为所有数据提供一个可信时间证明，确保各种数据可信，从而保障公司业务的可持续健康发展。

----------END----------

想联系我讨论此话题？请使用密信 App（ - ）扫码发加密邮件给我，我一定会回复您的加密邮件。