TSA

HSM时间戳服务器

不可否认的合格时间

HongKe 虹科

世界最快的加密时间戳设备

在任何可能造成财务影响或涉及人民安全的地方，或当工业4.0自动化按法律的规定执行功能时，合格的时间戳的重要性不亚于同步，因为它提供了事件的加密不可否认。

- 内含HSM
- 兼容RFC3161
- FIPS 140-2 Level3 Level4
- RSA 4096 bits
- X509 PKCS#11 PKCS#7
- SHA-256，SHA-2 MD5
- 合格的UTC参考时间

HongKe 虹科

www.hocyber.com

Elproma TSA 确保时间戳的防篡改创建和真实性。它是需要证明文档或数据在特定时间点的存在和状态的业务应用程序的理想硬件安全模块(HSM)网络设备。时间戳服务器(TSA)确保时间戳数据对于这些和类似的应用是真实的。时间戳能够随时验证，带时间戳的数据是否与时间戳记录的时间点上的形式完全一样。次外，时间戳(如果存在的时间比TSA长)仍然能够在没有TSA验证数据（文档文件或数据流）的情况下被验证：

1) *原创性*– 文件，视频流，图片等
2) *完整性*– 从数据被窃取时说什么也都没用
3) *年表的不可否认性*– 证明存在历史的瞬间

TSA的应用领域

- 长期的文件归档
- 电子认证/电子签名
- 招投标电子平台
- 税务局软件平台
- 公证和法律软件平台
- 彩票、在线投注和游戏
- 区块链/代币智能合约
- 新的加密货币系统，有限的花钱的时间
- 医药生产标签
- 疫苗的全球分销
- 食品、化学、水的全球分销

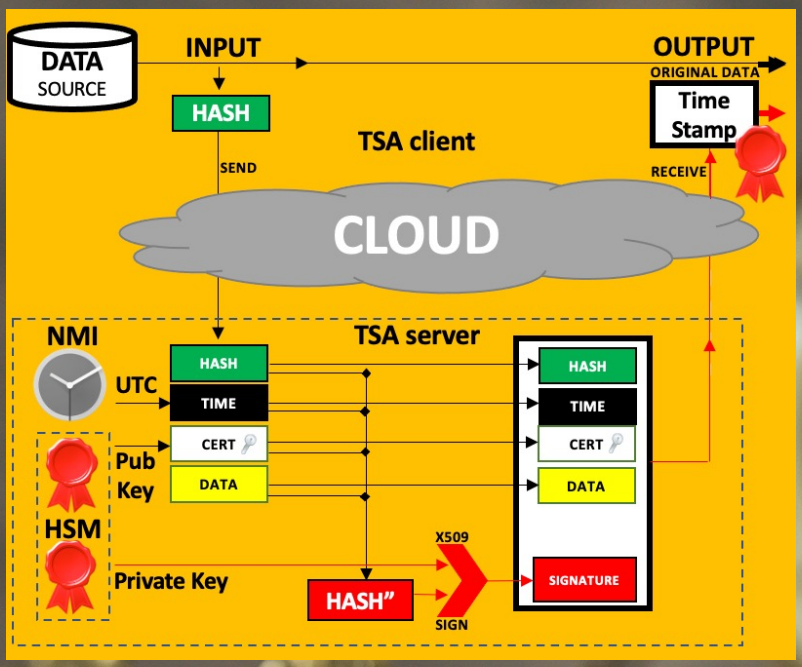
合格时间的重要性不亚于TSA使用的RSA算法的力量。目前，来自GNSS的时间非常容易被操纵，在时间戳中提供虚假的日期和时间。根据美国指令EO13905参考时间应该由NIST或国家计量研究所NMI提供。

HongKe 虹科

www.hocyber.com

PART #1 - 时间戳操作理论

任何数据的合格时间戳RFC3161过程都从客户端开始，客户端在其基础上形成一个[HASH]指纹，这是一个唯一的字节序列，用于“不可否认”的识别原始数据。指纹HASH的计算使用许多可用数学函数中的一个来执行；例如，SHA-256 或SHA-512 等。从现在开始，任何改变，即使是原始数据中的一个比特位的信息，都需要从一开始就开始操作。这就是所谓的“密封”信息，它是公认的数据属性完整性的功能的一部分。因此，在收到TSA (时间戳机构) 服务器发回的完整的RFC3161时间戳之前，原始客户端数据应保持不受干扰的原始形式等待。



[HASH]指纹被附加信息扩展，并通过网络发送到TSA 服务器。发送的数据流长度大约为500字节。它是使用HTTPS协议发送。在收到来自TSA客户端带有[HASH]指纹的请求后，TSA服务器对收到的数据进行补充，增加有关参考UTC日期和时间的信息[TIME]. 为了保证合格的时间戳，参考UTC应得到国家计量院(NMI) 的支持，使用经过认证的NTP 或IEEE1588协议。在一些限制条件下，参考UTC时间也可以从GNSS卫星上获得。根据US指令EO13905, GPS 一直处于干扰和欺骗攻击的风险中，因此使用它来同步关键基础设施需要再次追踪到NMI的UTC。在USA这一程序是由NIST负责的。下一步TSA添加带有公钥[CERT]和其他额外的[DATA]证书，并计算出准备好的反应的新指纹[HASH"]。最后，TSA从内部HSM(硬件安全模块)读取一个PRIVATE密钥，并对所有准备好的数据[HASH] + [TIME] + [CERT] + [DATA] + [HASH"]进行电子签名，创建合格的时间戳。结果通过网络发回给客户端，大约有1500字节，由客户端作为一个单独的文件与原始数据文件一起存储。

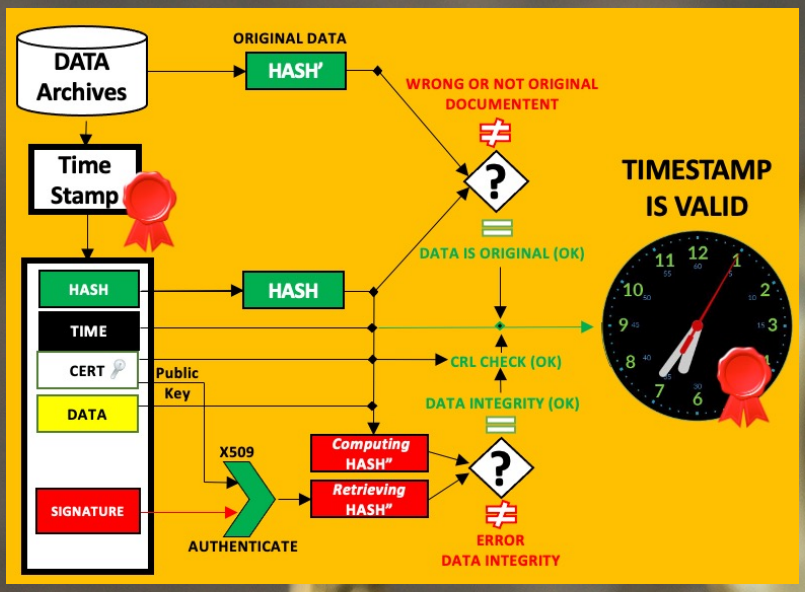
重要提示- 为了避免强RSA 加密器对虚假或篡改的日期和时间的影响，输入的UTC 参考时间应该可追溯到国家计量局。

PART #2 – 时间戳验证理论。

时间戳验证过程可以在任何时候执行，甚至在多年之后，而且验证不需要TSA服务器。为了验证，需要原始文档(文件、图片、视频)和包含证书及公钥的时间戳文件。验证过程包括测试TSA的身份(认证)和时间戳数据的完整性。它是通过使用证书[CERT].中包含的TSA公钥来完成的。

独立地，客户端从存储的原始时间戳数据中计算(重新计算)[HASH'] 指纹。如果它与检索到(先前发送的) 的[HASH"] 相匹配，则TSA认证和时间戳数据的完整性得到保留和可靠。否则，就会返回一个错误ERROR DATA INTEGRITY".

最后，需要检查验证的时间戳是否是指原始数据(文件),这基本上是验证过程的主题。因此，客户端根据原始数据(文件)的存档、未更改的副本重新计算新的[HASH']主要指纹代码，并将结果与从时间戳中获取的[HASH] 代码相比较。



只有这种匹配才能确保时间戳和原始文件的相互对应。通过这种方式，基于PKI属性、TSA认证、时间戳完整性、由时间戳可靠地指定的历史时刻文档以给定形式存在的不可否认性，实现了完整的验证。

重要提示 - 对TSA时间戳的回溯性成功验证并不能说明任何性能和准确的日期和时间。因此，建议你考虑保留额外的LOG文件档案，其中包含的信息可以被审计人员用来验证NMI的UTC 参考源的可追溯性。

HongKe 虹科

www.hocyber.com

合格的时间和GNSS的问题。今天，GPS 卫星信号仍然是最常见的时间来源。自1995年以来，民用工业逐渐采用GPS或其他基于GNSS的解决方案。随着时间的推移，IT行业拥有越来越多的卫星接收器，它们经常相互干扰(由于有源天线)。管理如此多的卫星接收器也变得很困难。首先出现了基于GPS同步异常的现象，导致IT系统出现故障。在越来越多的情况下，事实证明，由两个或多个独立的GPS接收器同步的相关IT系统出现时间差异，因此了提供了不同的RFC3161时间戳。这就造成了非常严重的问题。

GNSS的干扰/欺骗性攻击。此外，除了欧洲的GALILEO，其他所有的GNSS系统(GPS, GLONASS, BEIDOU, IRNSS)都是军事系统，根据地缘政治局势，不能保证接收到它们的信号。从GNSS收到的数据也可以很容易被操纵，从地球上制造虚假的发射。这就是所谓的欺骗。人们还可以干扰原始的卫星信号，这被称为干扰，或者故意延迟再重传(这就是它与干扰或信号反射的不同之处)，即所谓的模拟干扰(meaconing)。今天，行业的GNSS信号非常容易收到这种操纵和故意的网络攻击。对整个工业基础设施和对各国至关重要的基础设施的攻击也越来越多。

如今，同步与网络安全密切相关，因为– 与入侵内部网络相比，通过远程破坏同步过程来破坏整个IT架构的工作更加简单。如果系统易受其影响，那么剩下的破坏实际上就会随着而来。时间操纵可能会扰乱任何系统日志中记录的时间的业务、合同和时间顺序。在这种情况下，就会不可挽回地失去分析错误和确定故障的原因的机会，这就为黑客提供了理想的条件，转移了对故障背后真正的攻击原因的注意力。如今，整个网络安全模式已经改变，“ 时间同步攻击 ”和“ 时间延迟攻击 ”类的黑客攻击对于高度自动化、依赖GNSS的行业来说是最有可能和最危险的。

合格的时间参考是来自NMI

为了避免在虚假或篡改的日期和时间上使用强RSA加密算法，输入的参考UTC应该由国家计量研究所(NMI)提供。

技术规格

性能
- 每天400万个加密时间戳(365天24/7小时持续运行)
- 在负载峰值时，每秒钟最大100个加密时间戳
- 1GbE以太网(出厂默认) 2x接口标准
- 提供10GbE, 25GbE, 40GbE, 100GbE NIC可选项*

协议
- RFC 3161时间戳协议通过HTTP/HTTPS, TCP IPv4 & IPv6网络协议
- PTP IEEE1588, NTP SNTP, Chrony同步协议，带MD5认证

算法
- RSA, 密钥长度为2048, 4096,和可选的高达8192* 位
- Hash算法SHA-1, SHA-256, SHA-512, MD5

证书
- X509 PKCS#11和PKCS#7时间戳服务器证书支持

安全性
- 集成硬件安全模块HSM
- FIPS 140-2 Level 3
- FIPS 140-2 Level 4
- 符合ETSI规范TS102023

合格时间支持
- UTC可追溯到国家计量院
- UTC来自ELPROMA NTS-5000铷原子或铯原子钟
- DEMETRA* TSI#2 审计 &验证设施(可选项)

机械
- 1U rack'19标准机架
- 提供冗余电源100-240 VAC (最小功率60W最大功率300W*)
- 操作温度 +10°C to +50°C (存储温度 -10°C to +60°C)
- 湿度最高可达95%
- MTBF 300,000 hours 在25°C时

订货信息

Elproma TSA	(出厂默认) incl. 2x 1GbE ETH
Elproma TSA-10GbE	=> std. + 10GbE Ethernet Network NIC
Elproma TSA-25GbE	=> std. + 25GbE Ethernet Network NIC
Elproma TSA-40GbE	=> std. + 40GbE Ethernet Network NIC
Elproma TSA-100GbE	=> std.+100GbE Ethernet Network NIC

www.hocyber.com

HongKe 虹科