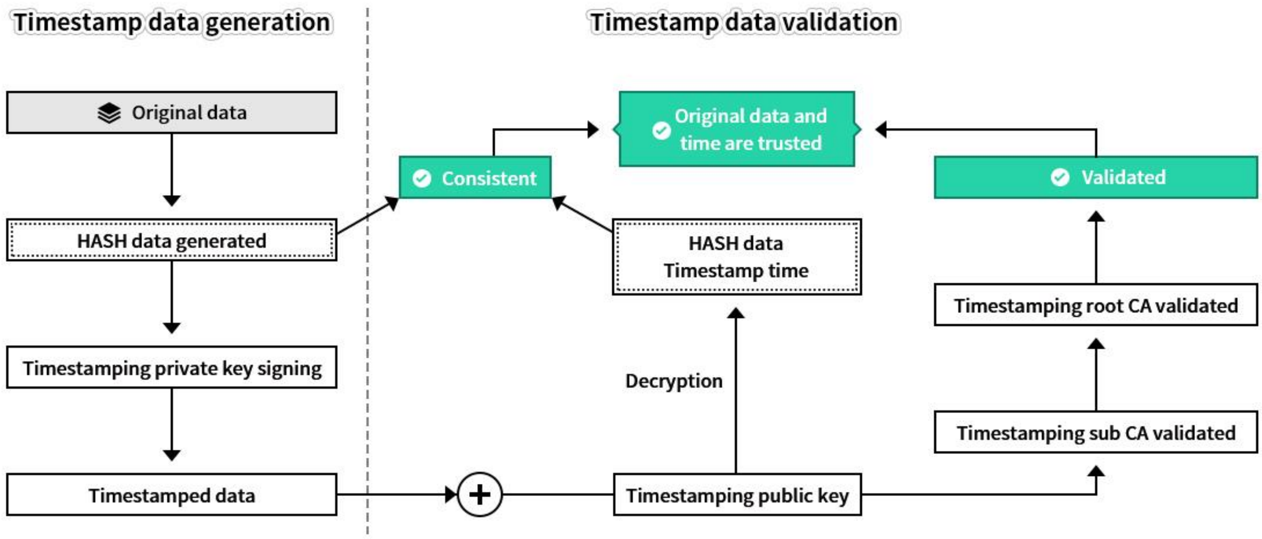
Timestamp, a Required Data Field in the Era of Big Data

（April 27, 2021）

What is timestamp? The timestamp is the signature data generated using digital signature technology. The object of the signature includes information such as original data, signature parameters, and signing time. The timestamp system is used to generate and manage timestamp data. The timestamping certificate is used to digitally sign the signature object to generate timestamp data to prove that the original data already exists before the signing time and cannot be modified afterwards, so as to ensure the record of the event time and data are all original data, which has not been modified.

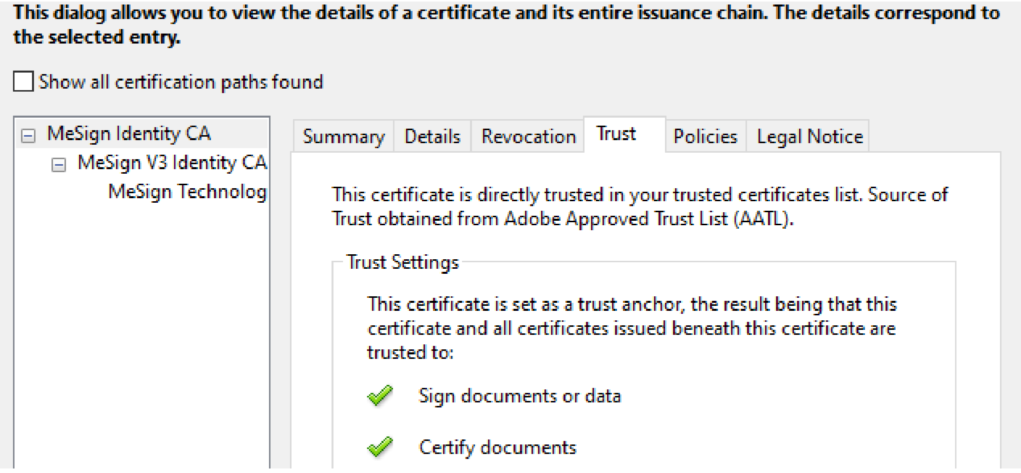
Now is the era of big data. The driving data of intelligent connected cars will be uploaded to the cloud. How to prove afterwards that the driving data is the original data and not the data "manufactured" by the manufacturer? The only feasible solution is to not only store the data itself when the data is generated, but also submit the data to a third-party timestamping service to obtain the timestamp signature data and store this timestamp data as a separate data field with the original data in the cloud database. In this way, if you need these data afterwards, you can export the original data and the timestamp data, and by validating the timestamp data, then the relying party can judge whether the original data at that time is authentic and trusted.

The principle of timestamp data generation and validation is shown in the figure below.


Timestamp data generation
Timestamp data validation
Original data
HASH data generated
Timestamping private key signing
Timestamped data
Consistent
Original data and time are trusted
Validated
HASH data Timestamp time
Decryption
Timestamping root CA validated
Timestamping sub CA validated
Timestamping public key

First, a cryptograph HASH is generated for the original data, and then a third-party timestamp service is called. The timestamp service system uses the timestamping certificate private key to sign the HASH data to generate the timestamp signature data. When you need to validate whether the original data is authentic, you only need to use the timestamping certificate public key to decrypt the timestamp signature data, calculate the HASH data of the original data and the trusted timestamp time, and then you can compare whether the HASH data of the original data in the database is consistent, consistent means that the original data has not been tampered with. Also use the intermediate root certificate that issued the timestamping certificate to validate whether the timestamping certificate is trusted, and then use the root CA certificate to validate whether the intermediate root certificate is trusted. If the certificate validation is passed, the third-party timestamping service is indeed used. Coupled with the consistent validation of the HASH data, it can be proved that the original data is trusted, it is the original one. As for whether the record time of the database is trusted, it should be based on the timestamp time, and the record time of the database is for reference only.

In fact, not only the car driving data, but also all CCTV data, hospital diagnosis and inspection data, public security and court data, e-government service approval data, etc., may need to be audited and checked in the future. How to prove that the data generation time is trusted and not-tempered afterwards, it is necessary to call a trusted third-party timestamping service to prove it. MeSign timestamping certificate has been strictly audited by WebTrust and has been trusted by Adobe. MeSign timestamping service is operated and maintained by 360 security cloud service to provide secure operation and maintenance services. The following figure shows the MeSign document signing certificate and timestamping certificate issued by MeSign Root CA is trusted by Adobe.



This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

This certificate is directly trusted in your trusted certificates list. Source of Trust obtained from Adobe Approved Trust List (AATL).

Trust Settings

This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to:

✓ Sign documents or data

✓ Certify documents

If you need to certify the trusted identity of the data producer, you also need to use the data producer's signing certificate to sign the data. The signature validation is same as the timestamp signature validation to validate the signer's identity to prove that this data is indeed produced by this user and confirm that the data is not tampered with, and the data production time is trusted by validating the timestamp signature data. That is, if only the timestamp signature service is used, the data is not tampered with and proves that the time is trusted; if it is also signed by the user's certificate, it can also prove that the data producer is indeed someone, this digital signature can be used to determine the right of data, this solution is for the application scenarios that need to prove data property rights.

To this end, the author urges all CIOs to take action to update the database structure of the management information system as soon as possible, add a timestamp signature data field, and purchase the MeSign timestamping service to provide a trusted time proof for all data. Ensure the trusted of big data, thereby ensuring the sustainable and healthy development of the company's business.

-- END --

Richard Wang

Digitally signed by Richard Wang
ceo@mesign.com

Want to contact me to discuss this topic? Please use MeSign App (👤 - ⛶) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.