GlobalSign®

Trusted Timestamping Services

RFC 3161 Trusted Timestamps

Long Term Signature Validation

GlobalSign's Trusted Timestamping Service provides a low cost and easy method to apply RFC 3161 trusted timestamps to time-sensitive transactions through independently verified and auditable data and UTC sources.

Timestamping services help organizations reduce the potential liability associated with time-sentitive transactions by providing a long term validation and non-repudiation of the time and date a transaction took place, using standards-based implementation that is easily recognizable and compatible.

Adding Trusted Timestamps allows organizations to:

-Add value to digitally signed or electronically signed documents
-Protect Intellectual Property
-Provide strong legal auditable evidence

Add Value to Electronic or Digital Signatures

Electronic signatures are deemed adequate for authentication of the author for many organizations and use cases. Adding a trusted timestamp provides a digital seal of data integrity and a trusted date and time of when the transaction took place.

Whether your organization uses electronic signatures for internal workflow processes or has developed trusted relationships with other organizations, GlobalSign's Timestamping Service can add significant value to your electronic signatures.

Recipients of documents with a trusted timestamp can verify when the document was digitally or electronically signed, as well as verify that the document was not altered after the date the timestamp vouches for.

-

Trusted Timestamps for Code

Many enterprises which are developing internal code are also implementing stronger processes around how code is checked in, verified as malware free and implemented. Part of the verification process can involve hundreds to thousands of dll, executable and CAB files that when run will produce signature validation long after the digital signature of the publisher expires.

Adding trusted timestamps to internal code that has been digitally signed with a self-signed code signing certificate provides enterprises with a timestamping service that is compliant with RFC 3161 to verify code long after the certificate expires.

Features & Benefits

- **Quick and easy to set-up with no technical expertise required**
  Simply incorporate TSA URL into your signing application

- **Recognized and compatible with various applications**
  Signatures are standard-based RFC 3161 compliant and already compatible with the most common systems and applications, including Microsoft and Adobe Acrobat

- **Legally admissible, secure non-repudiation signatures**
  GlobalSign Certificate Practice Statement (CPS) covers practices around Timestamping Authority (TSA) including private protection

- **SaaS-based Timestamping Model**
  GlobalSign manages all maintenance, security and audits 24 x 7

- **Document/Data Integrity**
  Timestamps include proof of data's existence within an exact point of time resulting in strong legal evidence

- **Standard-base Implementation**
  GlobalSign timestamps use standard-based implementation known as RFC 3161 with strong 256-bit hash algorithm

How GlobalSign's Timestamping Service Works

1. Implement GlobalSign timestamping URL into the client application such as Microsoft Office or Adobe Acrobat. The client connects to GlobalSign's TSA service and a hash is created.

2. GlobalSign TSA adds a timestamp to the hash and the signed hash and timestamp are sent back to the requester of the timestamp.

3. The client application receives the signed hash and timestamp and is recorded within the document or code.

For more information about GlobalSign solutions please visit www.globalsign.com | www.globalsign.co.uk | www.globalsign.eu