DigiStamp, Inc.

1.214.377.0378
www.DigiStamp.com
Dallas TX USA

Public Reporting of Policy Exception Event July 21, 2011

This memo states for public record an event whereby DigiStamp issued time stamps with an expired Audit Certificate.

The impact of this error is limited to the repairable condition of *having the wrong Audit Certificate* and does not invalidate the time stamp. Any timestamp issued with this error can be easily repaired by replacing with the correct, DigiStamp supplied, Audit Certificate. Only the Audit Certificate needs to be updated, the Time Stamp Public key certificate is correct.

There is no impact to DigiStamp's Subscribers or Relying Parties related to the security qualities of the time stamp. We anticipate minimal inconvenience to Parties who need to update the Audit Certificate supplied with the timestamp.

Impacted are time stamps created on Time Stamp node "TSA2" server using HSM denoted as "4758-95B00670 2005-07-07" during the period

From: 2011:07:12:18:29:39 Z
To: 2011:07:21:16:02:35 Z

Corrective measures have been taken to avoid this type of error in the future.

We apologize for any inconvenience.

Questions and concerns should be addressed to support@digistamp.com

The Board of Directors
DigiStamp, Inc.

Details:

The error impacted timestamps issued for users that had specific that the timestamp response should include a copy of the public key certificates.

As background, a timestamp is constructed as:

1. Time-Stamp Token - The time-stamp service returns a signed message in the standard form of Cryptographic Message Syntax, based on PKCS #7 version 1.5.IETF RFC 2630. A Time-Stamp Token contains the Signed Content and optionally public key certificates.

2. Signed Content - The signed message contains the time from DigiStamp's secure clock and the message digest of your document as defined in the time stamp x.509 PKI Time-Stamp Protocol IETF RFC 3161.

The error is that the timestamp included a copy of the outdated Audit Certificate. Based on PKI RFC 3161 standards the inclusion of the public key certificates as part of the time stamp data structure is optional. By design the certificates can be replaced or added at a later time without changing the validity of the time stamp (the Signed Content).

To resolve the problem for those timestamps created with this error is to replace the Audit Certificate in the Time-Stamp Token. The DigiStamp supplied replacement Audit Certificate is for the same public key but in a new x.509 certificate that has an extended expiration date. DigiStamp will provide the service of replacing the Audit Certificate to user who send us their timestamp and request this update.