

BEFORE THE
POSTAL REGULATORY COMMISSION
WASHINGTON, DC 20268-0001

)
Review of Nonpostal Services)
)

Docket No. MC2008-1

INFORMATION ASSURANCE CONSORTIUM MOTION (1) FOR LEAVE TO FILE A
LATE RESPONSE TO THE MOTION OF EPOSTMARKS, INC. TO STRIKE OR, IN THE
ALTERNATIVE, FOR LEAVE TO FILE SUPPLEMENTAL BRIEF (2) FOR LEAVE TO
FILE A RESPONSE TO EPOSTMARKS SUPPLEMENTAL BRIEF

(October 31, 2008)

For the reasons set forth in the attached document, the Information Assurance Consortium (IAC) respectfully requests the Postal Regulatory Commission (Commission) to allow the IAC to file a late response to Epostmarks, Inc. motion to strike IAC's Comments or, in the alternative, allow Epostmarks to file a supplemental brief. If the Commission allows Epostmarks supplemental brief to be entered into the record in this case, the IAC respectfully requests that the Commission allow it to file the attached document in response to Epostmarks supplemental brief. In the interest of fairness and completeness of the record, the Commission should allow the IAC an opportunity to respond to the new issues raised by Epostmarks supplemental pleading.

Respectfully Submitted,

Paul F. Doyle
Vice President
Information Assurance Consortium
PO Box 369
Ada, MI 49301
616-458-5733
paul@proofspace.com

October 31, 2008



October 31, 2008

Mr. Dan G. Blair
Chairman
Postal Regulatory Commission
901 New York Avenue, NW
Suite #200
Washington, DC 20268-0001

Subject: Docket MC2008-1

The Information Assurance Consortium (IAC), an all volunteer organization, apologizes to the Commissioners of the Postal Regulatory Commission for involving itself late in the process regarding Docket MC2008-1. The IAC leadership and members maintain responsibilities external to the IAC, including running individual, independent, for-profit businesses. Our providing input in the instant proceeding when we did (letter of September 30, 2008) was because we had only just become aware of the proceeding and the impending ruling. Our contributions are offered in a spirit of good will and in an attempt to provide beneficial information to the Commissioners as they progress toward their determination in this matter. We, the IAC, believe:

- There is a public need for Trusted Time Stamping services and solutions
- The market for Trusted Time Stamping can and will be built by private industry
- The IAC does NOT believe the USPS is necessary to the market, however we would not presume to preclude the USPS's participation if it were to be a responsible vendor

The business of securely operating a Trusted Time Stamping service, generating Trusted Time Stamps and providing these Trusted Time Stamps is a highly-specialized and very complicated technical activity. As we have reviewed the public record of this proceeding, we have several concerns:

- Have the Commissioners of the Postal Regulatory Commission been properly and fully informed by the USPS and other interested parties in the matter at hand?
- There are risks associated with the proper operation of a Trusted Time Stamping Service. These risks inure to the direct customers of the service and the public at large who may come to rely upon a Trusted Time Stamp procured by some other party.
- Has the USPS performed a proper risk analysis attendant to providing Trusted Time Stamping services to the wide consumer market? Performing risk analyses is considered necessary and appropriate for U.S. public entities and federal agencies? If the USPS has performed a risk analysis, why has this risk analysis and its findings not been made part of the public record? If the USPS has NOT performed a proper risk analysis, why not? Failure to have a risk analysis made part of the public record in this matter deprives the Commissioners of an essential piece of information necessary to making a well informed decision.

- The USPS has been well aware of the IAC and the concerns expressed by the IAC for several years. Why has the USPS not provided any of this information to the PRC as the USPS is perhaps one of the very best sources of information relevant to the matter at hand?

The IAC reminds the Commissioners that EPMS are simply a form of branded Trusted Time Stamp. The IAC recognizes the authority of the Postal Regulatory Commission to decide this matter. We do request that if the USPS is to be authorized to provide EPMS, they be required to do so in a secure, responsible and standards-compliant manner.

In regard to the motions filed by Epostmarks following the IAC's letter to the Commission on September 30, 2008, we wish to point out the following:

- Epostmarks is well aware of the IAC and our concerns with and objections to the USPS EPM program. In April of 2007, the IAC held extensive discussions with both Epostmarks and the USPS at their request (please see the accompanying copy of e-mail correspondence between the parties).
- Epostmarks appears to have not provided the PRC with all the information relevant to this matter. The information Epostmarks has provided appears to be selective and representative of a bias.
- Epostmarks by its own prior activities and correspondence can be said to have demonstrated that the IAC is an organization deserving to be heard and its positions to be given due consideration.

Finally, in response to some of the assertions made by Epostmarks in its motion to strike the IACs contributions, the IAC would like to remind Epostmarks that it is itself a very small entity.

The IAC maintains its invitation to the PRC to meet or speak by teleconference if additional input is desired.

Respectfully submitted,

Jeff Stapleton
President

Paul F. Doyle
Vice President

Tom Klaff
Board Member

Steven Teppler
Secretary

Doyle, Paul

From: Reck, Bradley A - Washington, DC [bradley.a.reck@usps.gov]
Sent: Tuesday, April 17, 2007 12:27 PM
To: Michael Wolf; Stapleton, Jeff; Adam Grossman; Klaff, Tom; Krappman, Paul; paul@proofspace.com; steppler@comcast.net
Subject: RE: IAC Call with USPS Monday at 1 PM

Jeff – I was looking back over a presentation that you made in February, 2004 at the RSA Conference entitled, “Trusted Timestamps... Truth or Consequences?” in which the conclusion lists the X9.95 standard documentation to include compliance evaluation criteria. I cannot locate this section in the X9.95-2005 document that USPS purchased in late 2006. Can you help me find the whereabouts of the [compliance evaluation criteria](#)?

-----Original Message-----

From: Michael Wolf [mailto:michael.wolf@epostmarks.com]
Sent: Friday, April 13, 2007 4:08 PM
To: Stapleton, Jeff; Adam Grossman; Klaff, Tom; Krappman, Paul; paul@proofspace.com; steppler@comcast.net
Cc: Reck, Bradley A - Washington, DC
Subject: FW: IAC Call with USPS Monday at 1 PM
Importance: Low

Gentlemen,

Here is a dial in number for the IAC call Monday with the USPS at 1 PM EST:

Guest Code	Toll Free	Direct Dial
495680	1-866-305-2467	1-719-387-4001

Adam and I will be on the call as well.

As an FYI and to help frame the discussion, I have included below an excerpt from the letter I sent to the USPS yesterday that relates to X9.95 certification for EPM Providers. I would like to thank Jeff for his excellent feedback and suggestions that helped me shape my recommendations on this important topic. We definitely would like to consider ourselves as members-to-be of the IAC and will be joining it as soon as we can (we are in the middle of a funding round).

I am hoping that during the call with the USPS, we can cover the following topics

- IAC recommended changes to “EPM Level 1 Service Provider Authorization process (aka “self certification)
- What other concerns, if any, do IAC members have with EPM program (i.e. involvement of Postal Inspectors) – Brad can provide some insights
- What other IAC members might be interested in joining EPM program if these concerns are adequately addressed? What timeframe?

If you have other topics you would like to discuss or feedback on my X9.95 recommendations I’m open to suggestions.

Mike.

-
- For the American National Standard X9.95, the normative Annex B of the standard describes a comprehensive set of twenty-two control objectives with several hundred evaluation criteria by which a Time Stamp Authority’s compliance to X9.95 can be evaluated by an experienced third party assessor. The USPS will need to review each of these control objectives and decide which are relevant to the USPS EPM program and which of those relevant controls should be evaluated by a third party. The USPS would then act as the authoritative body to interpret the Time Stamp Practice

Statements (for relevant self-reported controls) and third party assessment findings (for third party-evaluated controls) to determine whether the Time Stamp Authority can be certified as an EPM Provider on a pass/fail basis.

ePostmarks supports the concept of a third party assessment of the relevant controls from Annex B of the X9.95 specification for vendors that choose to use any one of the ANSI X9.95 methods in order to preserve the trust and integrity of the USPS EPM program. This assessment would be done by an assessor that is recognized by the USPS, with the USPS then issuing a Pass/Fail for the EPM Provider based on the report prepared by the assessor. It is worth noting that the majority of the controls in X9.95 are the same as those found in the Webtrust CA certification guidelines, so any reviewer that is familiar with Webtrust CA should be able to handle an X9.95 assessment.

Some compliance and certification programs in addition to a binary Pass/Fail evaluation also require that the assessed organization provide a remediation plan. This allows an organization to mitigate its risk over a reasonable timeframe. Also, since vulnerabilities and requirements change over time, such a process enables the USPS to properly manage its EPM program.

ePostmarks notes that the informative X9.95 Annex C describes and provides samples of Time Stamp Policy and Time Stamp Practice Statement that are comparable to those described above in RFC 3628. The European Telecommunications Standards Institute ETSI TS 102 023 V1.1.1 (2002-01) Policy Requirements for Time-Stamping Authorities was reviewed in the development of X9.95, as were RFC 3161 Internet X.509 PKI Time Stamp Protocol (TSP) and ISO/IEC 18014-1 Information technology – Security techniques - Time-stamping services. The USPS would develop and publish an X9.95 Time Stamp Policy for X9.95-compliant EPM Providers and then review and approve the X9.95 Time Stamp Practice Statements produced by each EPM Provider.

Sorry for the delay, but I needed to coordinate with Paul D. I'll be on the call, so if you can pass along the call-in information to me, that would be great. Thanks!

Paul K

From: Jeff Stapleton [mailto:jeff.stapleton@innove.biz]
Sent: Thursday, April 12, 2007 11:58 AM
To: Michael Wolf
Subject: RE: Call with USPS Monday at 1 PM

Mike,
 Are we on the call at 1pm Eastern? Do we have a dial-in number?
 Jeff

From: Michael Wolf [mailto:michael.wolf@epostmarks.com]
Sent: Wednesday, April 11, 2007 2:40 PM
To: Stapleton, Jeff; Adam Grossman; Klaff, Tom; Krappman, Paul; paul@proofspace.com; steppler@comcast.net
Subject: Call with USPS Monday at 1 PM

Gentlemen,

Jeff Stapleton suggested that a call with the USPS would be a good next step for the IAC in regards to the EPM program.

I spoke to Brad Reck from the USPS EPM program office and he is available to speak with us on Monday

at 1 PM.

Let me know if you have a dial-in number that you prefer to use, otherwise we can use ours.

Brad is interested in learning more about your recommendations for X9.95 certification; however his interest would be greater if any IAC members had submitted a letter of intent to actually be an EPM Provider. If you think your participation in the program is contingent on the USPS adopting different certification guidelines for X9.95-compliant solutions, this call would be an excellent opportunity to voice your concerns and also your potential support for (and participation in) the EPM program.

In the meantime, ePostmarks intends to submit a letter by Thursday in support of the idea of third party reviewers for X9.95-compliant providers. There are also other certification guidelines we will be mentioning in our letter that are appropriate for the other standards, such as RFC 3628 (ETSI TS 102 023) for RFC 3161, and UPU testing guidelines for UPU providers, that I won't go into detail about unless you are curious about them.

I would encourage you all to submit letters by the Thursday deadline as well, in order to give the USPS an indication of your support for the program if providers are appropriately reviewed and/or certified.

Regards,
Mike Wolf

From: Michael Wolf
Sent: Tuesday, April 10, 2007 1:05 PM
To: Michael Wolf; 'Stapleton, Jeff'; Adam Grossman; 'Klaff, Tom'; 'Krappman, Paul'; 'paul@proofspace.com'; 'steppler@comcast.net'
Subject: RE: IMPORTANT TO SCHEDULE CALL to discuss x9.95 assessment proposal for USPS

Gentlemen,

I'm hoping you all read the letter from the USPS and understand that we now have until Thursday to submit suggestions to the USPS for how to amend the certification process.

Adam sent out a meeting request for today (Tuesday) at 2 PM EST but I did not see any responses – is this call on? If so, is there a dial-in number? I can provide one if it will help.

Assuming the 2 PM does not happen, we are available today after 3 or Wednesday between 10 am and 2 PM EST. We really do need to have a call before Thursday to give everyone time to write their own letters to the USPS – if the IAC submits another BIDDER letter it will be ignored again because THE IAC IS NOT A BIDDER.

While we are getting the call set up, maybe we can continue this dialogue via email so we can make progress.

Since we spoke last week, I have solicited and received a proposal from Jeff Stapleton at Innove for doing an ANSI X9.95 assessment so I now have a better understanding of what is involved in this and how long it will take. The proposal is under NDA so I can't share it with you but I'm sure Jeff could provide each of you similar proposals under NDA if you were interested.

What would you think of the following proposal to the USPS:

- Since 3161 is included as part of ANSI X9.95, drop RFC 3161 as one of the accepted EPM Provider standards (so that only ANSI X9.95 and UPU S43 are acceptable)
- Propose that EPM Providers choosing the ANSI X9.95 standard must complete a 3rd party assessment of their controls by a third party vendor that is approved by the USPS and provide a copy of the assessment report to the USPS in order to go live with their EPM system.
- full-on X9.95 “certification” and periodic recertification being something that might come later as an official certification program is developed by some certifying body(or bodies) -AICPA/CICA and/or ANSI and/or IAC and/or ???.

Regards,

Mike Wolf

From: Michael Wolf
Sent: Friday, April 06, 2007 10:51 AM
To: Stapleton, Jeff; Adam Grossman; 'Klaff, Tom'; 'Krappman, Paul'; paul@proofspace.com; steppler@comcast.net
Subject: FW: x9.95 certification questions

Jeff,

Thanks for your informative response; it is helpful to begin to understand the nuances of "assessment" vs. "certification".

Have you ever done an X9.95 assessment? Has anyone? Any idea how long it would typically take? Are there levels of assessment (i.e., preliminary vs. full, or for "low value" vs. "high value" transactions)? Someone threw out figures like "40k to \$400k" and "weeks to months" on the call and I'm trying to calibrate what you would get for the low and high figures.

If we as a group are interested in proposing a "staged approach" to replace the "level 1 self-certification" and "level 2" proposed in the RFI might this look something like the following:

- 1) doing some type of "assessment" resulting in a pass by the USPS as a possible first step for bidders using the X9.95 standard to replace the "level 1 self certification" outlined in the RFI and
- 2) full-on X9.95 "certification" and periodic recertification being something that might come later as an official certification program is developed by some certifying body(or bodies) -AICPA/CICA and/or ANSI and/or IAC and/or ???.

I am trying to push this along quickly because I think the USPS may issue a letter inviting feedback as early as today and I think they are likely to set an aggressive deadline for responses (maybe as little as one week).

Mike

From: Jeff Stapleton [mailto:jeff.stapleton@innove.biz]
Sent: Friday, April 06, 2007 9:55 AM
To: Michael Wolf
Cc: Adam Grossman; 'Klaff, Tom'; 'Krappman, Paul'; paul@proofspace.com; steppler@comcast.net
Subject: RE: x9.95 certification questions

Mike,

Not to be too self-serving, but Innové does perform such security assessments. Because we are not an accounting firm, we do not perform "audits" per se, but rather assessments. Besides having developed the Webtrust for CA criteria (I used to work at KPMG) which is based on the X9.79 standard, the X9F4 working group (I am also the chair) has incorporated similar evaluation criteria in other ANSI standards, including:

- X9.79-2001 PKI Practices and Policy Framework
- X9.84-2003 Biometric Information Management and Security
- X9.95-2005 Trusted Time Stamp Management and Security
- X9.112-*draft* Wireless Management and Security – Part 1: General Requirements

Now, if you prefer an accounting firm with a CPA auditor, I can hook you up with Mark Lundin who runs the KPMG Webtrust for CA services. Mark and I worked together at KPMG and we were the original authors of the audit material in X9.79. He manages most of the CA audits in the US, including some very well known names. Only the X9.79 standard (a.k.a. Webtrust for CA) has been codified in an AICPA/CAC standard. The controls in X9.79 are exactly the same as Webtrust for CA; Mark did that work. The controls in X9.95 are 60% identical as X9.79: the IT controls and key management controls are the same; however instead of the X9.79 certificate management controls, the X9.95 standard has trusted time stamp controls.

Innové has a good history of performing security assessments of PIN-based payment systems for merchants, networks, and financial institutions as required by the PULSE and STAR networks. The controls for this type of assessments are based on X9.8 and X9.24 standards, organized in a separate X9 technical guideline called "TG-3." The payment networks do not require a formal audit, so non-accounting firms such as Innové are certified to do such work. Also, we are in the process of getting our PCI certification, another financial assessment program managed by the payment associations of Visa, MasterCard, Discover, American Express, and others.

The primary difference between an assessment and an audit is that the audit firm renders an opinion as to the existence and compliance of controls based on agreed upon criteria (e.g. Webtrust for CA). This opinion is either at a point in time (e.g. SAS 70 type 1) or over a period of time (e.g. SAS 70 type 2). Assessments provide their findings to the regulatory body (e.g. USPS) without rendering such an official opinion such that the regulatory body makes the pass-fail decision.

Another significant difference is that the auditor does not and cannot make any recommendations to the client on how to improve or fix a failed control. An assessor can not only make suggestions, but can assist in the design, development and implementation of improvements or fixes. I much prefer being an assessor and helping the client. Hope that helps.
Jeff

From: Michael Wolf [mailto:michael.wolf@epostmarks.com]
Sent: Thursday, April 05, 2007 5:09 PM
To: Adam Grossman; Stapleton, Jeff; Klaff, Tom; Krappman, Paul; paul@proofspace.com; stepler@comcast.net
Subject: x9.95 certification questions

Gentlemen,

I know some of you (Surety at least) are claiming X9.95 compliance with your solutions.

I am wondering, have any of you utilized a third party auditor, reviewer, assessor, or testing agency to test your compliance?

Can anyone recommend someone who could perform this type of service?

Is there a program for X9.95 similar to one run by the AICPA/CICA to license auditors for Webtrust CA?

In the absence of such a program, how can the USPS reasonably expect to authorize third parties to perform such an assessment?

Are the controls for X9.95 similar enough to Webtrust CA that a Webtrust CA-licensed auditor could perform them without much of a learning curve?

I am hoping to start an email dialogue that can be the start of some useful feedback or guidance that we, as a group, can provide to the USPS.

Mike Wolf

From: Adam Grossman
Sent: Thursday, April 05, 2007 5:27 PM
To: Stapleton, Jeff; Klaff, Tom; Krappman, Paul; Paul Doyle (paul@proofspace.com); stepler@comcast.net
Cc: Michael Wolf
Subject: USPS process update

Gentlemen,

I appreciate your time this afternoon and hope our efforts will bear fruit soon. I believe by working together as an industry we can influence the EPM program into a valuable asset for all of us.

I'm also writing to inform you that we spoke with the USPS this afternoon. They were responsive to our suggestion and we are expecting a letter from them shortly. Assuming it comes out in the next week I suggest we coordinate another phone call on Thursday or Friday.

Best regards,

Adam

Adam Grossman
[ePostmarks](#)
45 Euclid Street
Rochester, NY 14604
p: 585.546.4410 x150
c: 585.233.6929
f: 585.546.2269
ePostmarks.com