# Policy Proposal 2007-1

## Reinstatement of PGP Authentication Method

# Policy Proposal 2007-1 History

| | |
|---|---|
| Introduced on PPML | 25 OCT 06 |
| Designated Formal Proposal | 16 FEB 07 |
| First PPM Discussion | ARIN XIX |
| Last Revision | Not Revised |

Proposal Text In Meeting Packet
http://www.arin.net/policy/2007_1.html

# Policy Proposal 2007-1 Description

- Supports PGP authentication

**********

AC Shepherds

- Leo Bicknell
- Bill Darte
- Matt Pounsett

# Policy Proposal 2007-1 Legal Assessment*

**Comment:**

"Counsel has some concerns regarding liability that might be imposed on ARIN to by proposed policy 2007-1. These concerns may be resolved by explanation to cure my ignorance, or by editing if the concern exists. My most specific concern is that ARIN 'validate a chain of trust not longer than 5 steps"....I am concerned about fraud that may occur somewhere in the 5 steps that is not detected by ARIN. I have been told by techies that such an undetected fraud could easily occur. Does this policy leave ARIN responsible for damages to third parties, including our members, if it does not detect such fraud? It seems to me that establishment of an overall ARIN policy of cooperating in using PGP does not create this concern, but this specific language does. Is the additional language integral to PGP and hence unusual and unobjectionable? I apologize in advance if this is an instance where my lack of technical knowledge creates confusion."

* April 2007

# Policy Proposal 2007-1 Staff Comments*

- We recommend that a new NRPM section be created, "12. Communications", and that 12.1 be "Authentication". The subsequent numbering would change appropriately.
- The proposal uses the term "crypt-auth" as a notation to be affixed to POC records. Such notation is not technically necessary for ARIN systems to discern authentication methods, because mere existence of a stronger-authentication method than mail-from can (and currently does) automatically disable mail-from authentication.

* April 2007

# Policy Proposal 2007-1 Staff Comments (cont.)

- Staff believes that there was a formatting problem with the policy submission. It appears that the authors inadvertently incorporated procedural text under the headings "UPDATES TO TEMPLATES", "UPDATES TO DOCUMENTATION", and "KEY USE IN COMMUNICATION" under the policy text labeled "12.3 X.509: This section intentionally left blank." If passed without edit, such procedural text could be incorporated into the NRPM. Staff suspects this was not the author's intent, as these headings and their subsequent text are not numbered.
- In the section "KEY USE IN COMMUNICATION", the proposal requires validation of "a chain of trust not longer than five steps" between the signing key and ARIN's hostmaster role key, without regard to whether such intermediary signers are ARIN POCs, or are even known to ARIN. Without direct binding of the PGP key to an ARIN POC record, such anonymity in the chain of trust raises serious questions about how ARIN staff will know and evaluate that an e-mail from a signer is authentically from the ARIN POC that the sender claims to be.

# Policy Proposal 2007-1 Staff Comments (cont.)

- A PGP-key for hostmaster@arin.net exists on pgp.mit.edu as well as other well-known PGP-key repositories. This key was set up during the early days of ARIN, and the passphrase for the key is, as of this writing, MIA. This prevents ARIN from using the key to sign anything, and furthermore prevents ARIN from removing the key from the key repositories mentioned above. ARIN will need to generate a new PGP keypair, and publish the public key through the well-known PGP-key repositories. This is not a significant technical issue, but is mentioned because previous iterations of this proposal suggested using the original key, which is not possible.

# Policy Proposal 2007-1 Staff Comments (cont.)

- Currently ARIN uses two e-mail addresses, hostmaster@arin.net and reassign@arin.net, to accept e-mail. The purpose for the differentiation is primarily workflow-related: submissions to hostmaster are generally handled manually while submissions to reassign are generally able to be handled by automated software. PGP-key best practice dictates that each e-mail address have a separate key, and we would implement according to this practice. Staff notes that having two keys, and two addresses, may create opportunities for confusion or inadvertent misapplication of the wrong key to e-mails during functions like verification or encryption (i.e. use hostmaster's key to encrypt a submission to reassign). The concern is partially ameliorated by the fact that many MUAs will automatically select the proper key for encryption or verification based upon the e-mail address, but staff is aware that significant amounts of e-mail communication takes place outside of typical MUAs (e.g., c ustom scripts, etc.), leaving some degree of concern.

# Policy Proposal 2007-1 Staff Comments (cont.)

- The proposal text "ARIN shall PGP-sign all outgoing hostmaster email with the hostmaster role key, and staff members may optionally also sign mail with their own individual keys" implies that staff may sign with arbitrarily-sourced individual keys. We intend that if such keys are generated, they would be signed with ARIN's hostmaster key and controlled procedurally to maintain communication integrity between ARIN and its customers, including publication of those keys in widely-known repositories.
- NRPM Change – New section 12

# Policy Proposal 2007-1 Implementation Assessment*

- **Resource Impact: Significant**
- **Implementation: 4-12 months After BoT Ratification**
- **Implementation Requirements:**
  - Registration Software Changes
  - Template Changes
  - Directory Services Changes
  - Guidelines Changes
  - Staff Training

* April 2007

# Policy Proposal 2007-1
# PPML Discussion

- 11 for, 2 against
- Comments:
  - "It's fair to say that it is time we (membership) put PGP into play."
  - "Why is ARIN still using email for this process anyway? 1997 was a long time ago. The process is tailor made for a web app, perhaps with email confirmations, and such an app can be reasonably locked down irrespective of PGP. Worrying about email authentication entirely misses the mark."
  - "…under no circumstances should arin trust a message signed by a key not registered with arin through some business process."

| Posts | People |
|---|---|
| 118 | 21 |

# Policy Proposal 2007-1

http://www.arin.net/policy/2007_1.html