2007-1
Reinstatement of PGP Authentication Method

Paul Vixie
Mark Kosters
Chris Morrow
Jared Mauch
Bill Woodcock

12.2 PGP

ARIN accepts PGP-signed email
as authentic communication
from authorized Points of Contact.
POCs may denote their records “crypt-auth,”
subsequent to which unsigned communications
shall not be deemed authentic
with regard to those records.

Arguments in Favor:

- Provides authentication for communications between ARIN and POCs
- Protects our resource records against hijacking and vandalism
- Does not change or remove any current services
- Brings ARIN's service level up to that of the other four RIRs
- Restores a service which was previously available under the InterNIC
- Keeps us from looking like idiots who can't figure out basic crypto

Arguments Against:

- PGP "Web of Trust" might fail, and cause ARIN hostmasters to authorize the wrong parties to modify records.

  False.

  This confuses or conflates AUTHENTICATION and AUTHORIZATION. This proposal does not modify the mechanism whereby ARIN AUTHORIZES POCs in any way. It merely uses the most widely-established mechanism to cryptographically AUTHENTICATE them, assuring their identity.

Arguments Against:

- It would be easier or better to invent some new authentication protocol or process from scratch, perhaps involving web transactions.

  False.

  PGP has been the most widely used protocol for digitally-signing communications for more than fifteen years. It is an open IETF standard (RFC2440), with many interoperable implementations. It works fine in the rest of the world, and it worked fine here prior to ARIN. Furthermore this is not an either/or proposition; this proposal in no way precludes the implementation of other authentication methods.

Arguments Against:

- ARIN hostmasters have lost the passphrase for a private key associated with hostmaster@arin.net. Therefore, ARIN can no longer use PGP.
  False.

  This presents no impediment to implementation.

  A new key can be generated, covering that, and any other email addresses ARIN wishes to use for official communication.

Arguments Against:

- If this proposal were passed, it would require ARIN resource recipients to do something differently.

False.

This proposal does not place any requirements upon resource recipients. It does not change or remove any current services. It merely reinstates one service, which ARIN resource recipients may use if they so choose.

Arguments Against:

- Without direct binding of the PGP key to an ARIN POC record, ARIN staff won't know that an e-mail is from the authentic POC.

False.

This arises from misunderstanding of public/private key cryptography as implemented in PGP. Only the authentic POC possesses the PGP private key of the authentic POC, and the normal PGP authentication mechanisms provide transitive trust. There is no need for ARIN to reinvent cryptography before using it, any more than it need reinvent email to be able to use it.

Suggested Modifications:

- The “crypt-auth” notation is not technically necessary for ARIN systems to discern authentication methods.

  No problem.

  The authors merely used this phrase to convey the intention of the policy. Since there should be no publicly-visible indication of the protection method in place anyway, no descriptive phrase is needed.

Suggested Modifications:

- Currently, the suggested implementation requires that staff reject any PGP signature with a minimum transitive distance greater than five steps. This may be overly prescriptive.

  No problem.

  This was merely a suggestion, and yes, it would probably be better to leave the judgment of the quality of a path to the discretion of staff, provided that they not arbitrarily reject reasonably multiply-signed keys at reasonable distances.