NTP Autokey Draft
draft-ietf-ntp-autokey-00.txt

Brian Haberman

IETF 70, Vancouver
Status

• WG Last Call started 2007-11-02

• One set of comments received 2007-11-15 (Thanks Danny)
  – Issues described in following slides

• Dave provided some resolutions 2007-11-19
Missing Field Descriptions

• Section 10.5 is missing diagrams specifying field layouts
• Field description text is good, diagrams needed to orient layout in extension field

• Resolution: Document editor needs to draw these diagrams
NAT Traversal

- The described protocol will not operated through a NAT
- Need shared set of identifiers that are not typically available to both ends
- Proposed resolution: Remove paragraph discussing NATs
Certificate Retrieval

• Text is unclear which server is being used to retrieve a certificate
• Does a client need to follow the certificate chain?

• Proposed resolution: Unclear. Dave’s response does not appear to resolve the issue.
Certificate Trails

- Text currently says a masquerading attack on client certificates can be mitigated by reverse-DNS
- Text is supposed to address a rogue server not using an identity scheme
- Proposed resolution: Remove sentence discussing the use of reverse-DNS. Unclear to the editor if that addresses the whole issue.
NTP Filestamps

- Text in section 8 refers to filestamps, but there is no description of how they are created or why it is used.
- Appendix A describes filestamps and how they are created.

- Resolution: Add forward reference in section 8 to Appendix A.
Signature Coverage

- Section 8 says “The signature covers the entire extension field, including the timestamp and filestamp, where applicable.”
- Unclear that it only covers the extension field
- Resolution: Clarify text to explicitly state that the signature only covers the extension field.
IFF Confusion

• IFF used to identify Schnorr Identity Scheme and as a status bit indicating confirmed credentials

• Resolution: Rename the status bit to another acronym. Suggestion?
Filestamps in Extension Field

• Figure 9 shows filestamp and timestamp fields but text does not describe how they are obtained.

• Proposed resolution: Forward reference to Appendix A.
Lighting Error Bits

• Protocol description does not discuss all conditions for lighting error bits
• Reference implementation has “literally hundreds” of conditions causing error bits to be lit

• Resolution: No change since this is an Informational document
Gethostname() Assumption

• Protocol use of gethostname() assumes a minimum of 4 and a max of 256 characters

• Proposed resolution: Change min to 1 and leave max as 256.
CERT Message Use

• Is the CERT message only used between a client and a single server or the server chain?
• Validity of signature since self-signed?

• Proposed resolution: Clarify that client follows the chain and that validity is determined by identity scheme in use
Leapseconds Table

- Table diagram needed to describe Leapseconds message format

- Resolution: Add figure with Leapseconds message format
Autokey Version Number

- Security Considerations section discusses “compatibility with previous NTP versions”.
- Text is actually discussing compatibility with previous Autokey versions.

- Resolution: Clarify text to state “compatibility with previous Autokey versions”.
IANA Registry

• IANA Considerations section requests creation of Autokey Message Types and Autokey Scheme Types
• Given the Informational status of the draft, can these registries be created?

• Proposed resolution: Remove the registries. Does this hinder the ability for two implementations to inter-operate?
Editor’s Next Steps

• Fix all the nits identified by Danny
• Revise draft based on resolutions discussed here
  – More than willing to hear alternative solutions
WG’s Next Steps

• Document cannot be advanced with a single reviewer’s comments
• NTPv4 protocol specification cannot advance with the Autokey specification

• REVIEW!
  – Provide comments or
  – Indicate your happiness with the draft