DISPATCH
@IETF123

RFC 4130 Specification Update

draft-petta-rfc4130bis

Debra Petta (Drummond Group)

Motivation

- *AS2 is a popular and highly adopted protocol used by the Retail, Healthcare, Financial, Logistics and Oil & Gas sectors*
- *RFC 4130 is the authoritative specification, but it is over 25 years old.*
- *Security requirements have changed, and guidance on best practices needs to be included.*
- *New features that many AS2 providers have already implemented are missing from the standard.*
- *The AS2 user community is asking for updates to be made.*

Background

New AS2 implementations rely on RFC 4130 during their design, development and QA process, however it is out of date and is missing the details needed to make it interoperable with existing AS2 implementations that have evolved to support new requirements.

For the AS2 specification to maintain its authority and trust in the user community, it needs to have:

- *Updated references to more secure algorithms and removal of the deprecated algorithms*
- *Inclusion of new features created to support industry needs*
- *Clarification and resolution of ambiguities in the standard*
- *Guidance on best practices that will help with interoperability*

Summary of Needed Changes

- *Signature hashing algorithms (MD5, SHA1) updated to SHA2*
- *Encryption algorithms updated from 3DES to AES*
- *Removal of references to AS1 and encodings for SMTP transmission*
- *Suggested security best practices, e.g., HTTPS, usage of TLS 1.2 (or greater), removal of insecure SSL versions and cipher suites, guidance on certificate creation and usage, etc.*
- *Clarification of rules for usage of specific MIME headers (e.g., AS2 System Identifiers, Message Identifiers, etc.)*
- *Documentation of additional MIME headers that are either already in use or would augment the AS2 developer and end-user experience*
- *Description of additional AS2 features: CEM, AS2-Reliability and Restart, Multipart-Attachments, Filename Preservation, etc.*
- *Updated example messages*

IETF

Current and Expected Interest

- *Large AS2 vendors (e.g., Amazon, IBM, Oracle) regularly engage with us for guidance and have expressed concern regarding the interoperability of their products with other products that use the current version of RFC 4130.*
- *We have assembled an internal advisory group from some of these companies and other interested parties. They have provided us with a "wish-list" of specific things they'd like to see changed.*
- *A very detailed list of proposed updates was recently shared to the ART Area and Dispatch email lists for review and comments.*
- *We have encouraged the members of our advisory group to participate in these discussions.*
- *We also hope to recruit others from the IETF community to join in these discussions.*

Hoped dispatching outcome

RFC 4130 was part of the EDIINT working group.

Since we are proposing to obsolete RFC 4130, which is an existing standards track document, our hope would be to either:

- *Reopen the original EDIINT working group, or*
- *Form a new working group*