Database of Long-Lived Symmetric Cryptographic Keys

draft-ietf-karp-crypto-key-table-08

R. Hously

housley@vigilsec.com

T. Polk

tim.polk@nist.gov

S. Hartman

hartmans@painless-security.com

D. Zhang

zhangdacheng@huawei.com

Changes since IETF 86

- Updates for Genart review
- Updates for routing directorate review
- Awaiting IESG ballot

Internationalization

- Key names could be strings; complexity results if they contain international characters
- KARP's uses never anticipate this issue; theoretical problem for our usage
- Require any protocol that has i18n issues to deal with them

Internationalization Text

Typically

this field does not contain data in human character sets requiring internationalization. If there ever are any Protocols with key names requiring internationalization, those specifications need to address issues of canonicalization and normalization so that key names can be compared using binary comparison.

Admin Key Name

- As an editorial error, the admin key name was not added to the document after the group agreed to add it
- A reviewer noticed that there was no unique name for managing keys
- Actually added this time

Clarify Protocol Specification Role

- Protocols need to define form of key names
- Clarify boundary between protocol and key table
- Old text: “protocol may restrict”
- New text: “protocol defines the form”

- Packet becomes message everywhere
- Clarify interfaces is not protocol specific; use peers when it is
- IANA registries improved thanks to our chairs