

IANA Rules for MIKEY

draft-arkko-mikey-iana-00

J. Arkko, A. Keränen, J. Mattsson

IETF 80, Prague

March 29th, 2011

Ari Keränen

Background

- MIKEY (RFC 3830) and its extensions define a set of namespaces handled by IANA
 - Next payload, PRF function, MAC algorithm, etc.
- Most of the namespaces have two parts
 - Assigned through IETF Review (i.e., need IETF RFC)
 - Reserved for private use (i.e., IANA doesn't track)

Background

- IETF Review (as the only option) has turned out to be unnecessarily strict requirement for reserving values for most of the namespaces
 - Special circumstances may justify lighter process on a case-by-case basis
 - E.g., independent submissions, IRTF RFCs, etc.
- Multiple RFCs have had the same problem (and similar fix)

Proposed Changes

- Changing “IETF Review” into “IETF Review or IESG Approval” for the following namespaces
 - Next payload, PRF func, CS ID map type, Encr alg, MAC alg, DH-Group, S type, TS type, ID type, Cert type, Hash func, SRTP {Type, encr alg, auth alg, PRF}, FEC order, Key Data Type, KV Type
- IESG Approval: judgment call by the IESG if document warrants an allocation

Proposed Changes

- Changing “IETF Review” into “Specification required” for the following namespaces
 - Prot type, Error no, General Extension Type, KEY ID Type, OMA BCAST Types

Other (Fixes)

- In addition, making small clarifications/fixes to the MIKEY IANA registry
 - Value ranges are incorrect for some namespaces
 - Sub-registry names are not consistent
 - Version registry was missing
- Not changing rules for other registries
 - Version, Data type, C envelope key cache indicator
 - TS Role, ID Role, RAND Role, Ticket Type

Next Steps

- WG or AD-sponsored document?
- Comments are welcome!