IPsec in IPv6 Node Requirements
draft-ietf-6man-node-req-bis-05.txt

Thomas Narten
narten@us.ibm.com
July 29, 2010
IETF78 – Maastricht
SAAG
IPv6 Node Requirements

- RFC 4294 (IPv6 Node Requirements) says:
  - IPsec Architecture (RFC 4301) is a MUST
    - Implies IKEv2 is a MUST
  - But 4294 says key management is only a SHOULD

- Problems with the 4294 recommendation:
  - Key management recommendation is mushy/contradictory
  - IPv6/6man WG has never been comfortable with making IKEv2 a MUST for ALL devices
  - Doesn't reflect reality: many devices with IPv6 choose not to include IPsec & IKEv2; MUST language won't change that
  - Mandating IPsec without mandating IKEv2 seems wrong
  - Classes of devices (e.g. constrained) exist for which other security mechanisms are reasonable choices

- Proposed Revision: make IPsec AND IKEv2 (strong) SHOULD
  - Include more text with practical guidance and context
What MUST/SHOULD Means

- MUST/SHOULD as defined in RFC 2119 says:
  
  1. MUST   This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
  
  3. SHOULD   This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
  
- MUST is absolute: no exceptions
  
- SHOULD is the right keyword when exceptions need to be made
Questions/Comments?