Internet Standards Conflicts

Russ Housley
IETF Chair

Bernard Aboba
IAB Chair

10 March 2013

Introduction

- IETF, IEEE 802, and W3C develop standards that are very important to the Internet
- For all three organizations, there are conflicting specifications for a few standards submitted to “formal standards bodies”
- Varying interpretation of WTO rules is a contributing factor
  - US: international market-determined standards set by non-governmental bodies are acceptable as mandatory
  - EU, China, Korea, etc.: Only formal inter-governmental bodies (e.g., ISO, ITU-T) are acceptable as mandatory
- Seek a way to …
  - increase the effort to submit a conflicting specification
  - reduce the effort to get nations to support the multi-stakeholder standards

IEEE 802 / ISO Relationship

- IEEE 802 historically submitted some standards to ISO for ratification
  - ISO 8802 series of documents contains the ratified standards
  - W3C now (selectively) taking this approach
- Many documents in the ISO 8802 series are obsolete or significantly out of date
  - IEEE 802.3 WG explicitly requested withdrawal of ISO 8802-3:2000
  - Considering a proposal to withdraw the whole series

Questions Raised This Proposal

- Is it important for an IEEE 802 standards to be recognized as “international” and thus protected by international trade treaties?
  - Does the WTO consider an IEEE 802 standard to be international?
  - Do all countries recognize the an IEEE 802 standard as international?
- Is there any additional value in submitting IEEE 802 standards to ISO for ratification?
  - What is the value to IEEE 802 and national bodies?
  - Do we expect any technical value?
  - Are the answers different for each IEEE 802 WG?
- How should IEEE 802 submit standards for ratification?
  - Using the PSDO method or the fast track method?

IETF / ISO Relationship

- IETF does not submit standards to ISO for ratification
  - Submission of standards-track RFCs would incur a large cost; benefit thought to be insufficient
- Liaison relationship
  - More than a decade ago the IETF requested Class A liaison relationship with ISO
  - IETF request was rejected; however, ISO offered a Class C liaison relationship instead
  - IETF rejected this counter offer
  - Ultimately, ISOC on behalf of the IETF was given Class A liaison relationship with ISO/IEC JTC1/SC6

Liaison with ISO – 2nd Try

- About a year ago the IETF Chair informally talked to the JTC1 Chair about a Class A liaison relationship with ISO/IEC JTC1
- JTC1 Chair offered an agreement that would “fast track” the assignment of ISO numbers to IETF standards
- IETF Chair rejected this counter offer

  Note: W3C has taken this approach for some of their standards to reduce likelihood of competing standards from national bodies

Conflict Storyboard

- Specification becomes a national standard
- National standard submitted to ISO or ITU-T for “fast track” processing
  - No check for collision with multi-stakeholder standards bodies
  - Big effort required to educate governments about the impact of these collisions with IETF or IEEE 802 standards
- Rapidly goes to ballot by nations
- Unclear how many nations will follow this storyboard
- Security seems to be drawing attention at the moment

IETF Support for National Cryptographic Algorithms

- IETF creates few obstacles to support of national cryptographic algorithms in IETF protocols
  - Public pointer to algorithm definition required, but the documentation need not be an RFC.
  - Easy to publish specifications on algorithm use with IETF security protocols as Informational RFCs
  - Procedures in place to allocate code points
  - Process already used for publication of RFCs specifying use of US, Korean, Japanese, and Russian cryptographic algorithms

USA – Suite B – RFC 5430, 5647, 6239, 6318, 6379, 6380, etc.
Korea – SEED – RFC 4009, 4010, 4162, 4196, 4269, 5669, 5748
Japan – Camellia – RFC 3657, 3713, 4132, 4312, 5528, 5529, etc.
Russia – GOST – RFC 4357, 4491, 5830, 5993, etc.

Conflicts in ISO

- WAPI
  - Fast track approval requested in ISO/IEC JTC1 for alternative to IEEE 802.11i (WiFi Security)
  - Proposal included Chinese proprietary encryption and key management
  - Major effort by IEEE 802 to prevent document approval
- Current flash point: ISO/IEC JTC1/SC6
  - Specifications submitted using Chinese cryptography
    - **NuFront –** new 802.11 PHY and MAC
    - **TePA-AC** – LAN security – Alternative to IEEE 802.1X
    - **TLsec** – LAN security – Alternative to IEEE 802.1AE
    - **TAAA** – Alternative to IEEE 802.16 security
    - **TIsec** – IP security – Alternative to IETF IPsec

IETF Response to TIsec

- Discussion with IEEE 802 Leadership
- IAB and IESG sent a liaison statement to ISO/IEC JTC1/SC6
  - Please do not develop an alternative to IPsec
  - Assignment of a protocol number to such a development would be difficult
  - Better to specify use of Chinese cryptography with IPsec

Observations & Summary

- Asian nations (and others) prefer one-nation-one-vote environment
  - Huge effort is needed for an SDO to convince each government to cast their vote in a particular manner
  - Most governments are reluctant to get involved in a standards dispute; standards not considered an issue for diplomatic energy

Summary: Small effort for a nation to submit a national standard for fast-track processing, but a major effort is required to respond

Backup Slides

Summary of IEEE 802 Discussion on ISO Ratification

- There was consensus that it was important for IEEE 802 standards to have “International” status
- There was an understanding that IEEE 802 standards are not considered to be “International” by many countries
- On that basis, IEEE 802 WGs should consider on what basis and under what conditions they might send IEEE 802 standards to ISO for “registration”
- Concerns were raised that the PSDO agreement might allow ISO to agree to make modifications to the ratified document
  - Want all modifications to use IEEE 802 processes
  - Might be possible to negotiate between ISO/IEC JTC1/SC6 and IEEE 802

Summary of IEEE 802 Discussion on ISO Ratification

- Like to avoid ISO/IEC JTC1/SC6 duplicating IEEE 802 functionality
  - This is a more difficult issue because national bodies always have the right to make standards
  - ISO/IEC JTC1/SC6 standards should avoid adding functionality to IEEE 802 standards without agreement from IEEE 802

SC6 National Bodies

- SC6 P-Members
  - **Korea – KATS**
  - Spain – AENOR
  - France – AFNOR
  - **USA – ANSI**
  - **UK – BSI**
  - **Germany – DIN**
  - Greece – ELOT
  - Russia – GOST R
  - Luxemburg – ILNAS
  - Tunisia – INNORPI
  - **Japan – JISC**
  - Kazakhstan – KAZMEMST
  - Kenya – KEBS
  - Belgium – NBN
  - **Netherlands – NEN**
  - **China – SAC**
  - **Canada – SCC**
  - **Finland – SFS**
  - Switzerland – SNV
  - Czech Republic – UNMZ