draft-ietf-ntp-using-nts-for-ntp-06

D. Sibold

NTPWG Interim Meeting,
14th October 2016, Boston

In WG Design Team discussed Items

	Item	Status
1	Mandatory to implemented KE	Agreed – DTLS - Over separate Port - Piggybacked on NTP header
2	Are optional KE mechanism allowed?	Open
3	Two-way authentication	Agreed - Second tier effort - KE must be able to support mutual authentication
4	Authorization	Agreed - Second tier effort
5	Broadcast mode	Agreed - Second tier effort However PTP needs broadcast/multicast mode!

In WG Design Team discussed Items

	Item	Status
6	Chicken-egg problem	Agreed – Discussed in the section “Security considerations”
7	Unauthenticated time packets	Agreed – MUST NOT be applied for time synchronization. - Discussed in section “Security considerations”
8	Cryptographic agility	Agreement that cryptographic agility is needed A minimum list of mandatory mechanisms shall be provided Message Authentication Code - GMAC shall be provided because of performance advantages - HMAC shall be provided especially for embedded devices
9	Cipher suite selection	TBD - Daniel proposal already contains language on

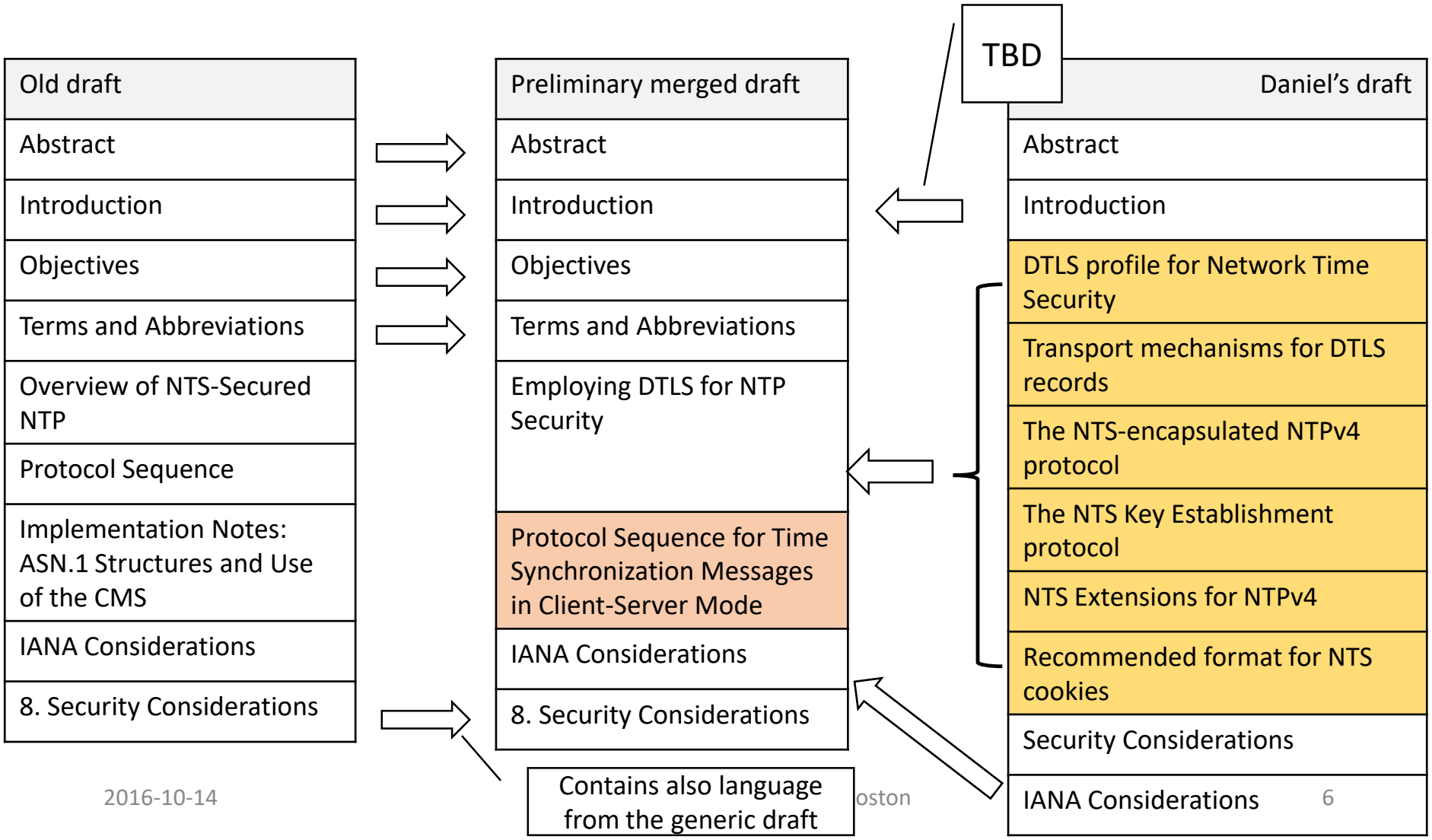
In WG Design Team discussed Items

	Item	Status
10	Privacy	Open - New requirement (not included in RFC 7384) - Not final agreement

In WG Design Team discussed Items Summary of open items

	Item	Notes
	Are optional KE mechanism allowed?	
	Privacy	If yes, is the current approach suffient?

Merge of NTS for NTP draft with new proposal



Merge of NTS for NTP draft with new proposal

- TBD
  - Final specification of the protection of time request and response messages
    - Depends on the privacy requirement
      - Also important for the section “Objectives”
  - Text from Daniel’s introduction
  - Text from Daniel’s essay for the security consideration
- If optional KE mechanisms are allowed:
  - Current DLTS based KE should exchange key(s) and state information as application data
- Broadcast mode has been dismissed