Questions about the Transport of Intercepted IP Traffic document

Q1. Which version is the standard according to the law (V0.1.2 Draft or V0.2.0 Standard)?

Q2. May lower versions of the TIIT be implemented?

Q3. What is the procedure according to changes of the TIIT? How are changes made? Who takes care of communications of changes? When en how are changes technically implemented?

Q4. Piii: What means “functional unit”? When this is the S1, S2, T1 or T2 is seems that S1 and S2 or T1 and T2 may not be combined. Is this correct?

Q5. What means LEMF? Is this only the combination T1 + T2 or also S1 + S2?

Q6. P1: Are the S1+S2 combination meant by “interception function”? This means that TIIT only specifies the handover interface between S2 and T1. Is this correct?

Q7. Where can I find or get the documents in the References?
A. [Bra97] RFC2119: ftp://ftp.ietf.org/rfc/rfc2119.txt
[CLE+00] Functional Specifications: Can be obtained via the Ministry of Justice or the Dutch ISPA (NLIP).
[DA99] RFC2246: ftp://ftp.ietf.org/rfc/rfc2246.txt
[Mil92] RFC1305: ftp://ftp.ietf.org/rfc/rfc1305.txt
[RV00] AMvB: unknown yet
[Sri95] RFC1832: ftp://ftp.ietf.org/rfc/rfc1832.txt

Q8. Are all these documents available in English?

Q9. P4: What (kind of) personnel (on the ISP-side) are involved in Lawful Interception?

Q10. P4: How about subcontractors having (a part of) the network in control. Are employees of the subcontractors authorized personnel?

Q11. P4+6: Will there be any transport media other than the Internet (in the future) for LI?

Q12. Is it necessary to record log events for LI even when in normal operation this is not done?

Q13. Are hosting companies also ISP within this context (only having a server but no network services)?

Q14. P7: Can a “normal” network within a building connecting S1 and S2 be marked as a secure channel? On page 14 is stated that a secure channel is not necessary if S1 and S2 are in the same building. Is this correct? Is encryption necessary when S1 and S2 are in the same building (Page 8)?

Q15. P7: Is an encrypted channel over the Internet possible to connect S1 to S2?

Q16. P7: What is the C2 protocol / channel?

Q17. P8: What margins of the time are allowed? E.g. can S2 be synchronized with NTP from the Internet and act as a NTP server for S1?

Q18. P8: What are all these acronyms?

A.	ISP	Internet Service Provider
	Interception Function	?
	NTP	Network Time Protocol
	SNMP	Simple Network Management Protocol
	DPDU	?
	PDU2	?
	SHA (hash)	?
	TIIT	Transport of Intercepted IP Traffic
	SSL	Secure Socket Layer
	TLS	?
	TCP/IPSec	?
	IKE	?

Q19. P8: Why MUST S1 generate the hash? May S2 do this job? S1 can be a standard machine in this case, without modifications.

Q20. P9: How does S1 function anyway without an IP stack? An IP stack is necessary to monitor to IP traffic! How is IP stack defined in this situation? (having an IP address?)

Q21. P9: What is the procedure when S2-T1 communications times out?
E.g. who are authorized personnel? How do you know for sure (on the other side)? Receiving side contacts are not specified in the XML-example! How to reach the LEA? By phone? How to secure this communication channel?

Q22. P9: Is TIIT meant as a RFC? If so, why is it not formatted as such?

Q23. P9: What kind of alarm is possible to alarm authorized personnel when a crypto suite is not correct? What must the personnel do next?

Q24. P9: Which crypto suites are allowed?

Q25. P12: definition of "int". Is this 32 bit?

Q26. P13: Who or where is the Sniffer ID determined?

Q27. P14: MUST S1 encapsulate the PDU's or may S2 do this job?

Q28. P14: When T1 cannot reach any T2 there traffic from S2 will not be accepted. This means that after one hour the ISP personnel has to inform the LEA personnel. Should there not be a mechanism that the LEA-personnel informs the ISP? E.g. the T1 – S2 should also have a time-out and procedure of contacting the ISP.

Q29. P14: Does the S2 has to buffer the traffic when a link (S2-T1 or T1-T2) is not available or even down?

Q30. Is there a difference in channel status (status="down") between S2 and T1 when a time out occurs of 300 s. (retries) or 3600 s. (alternative route)? MUST the traffic that is received by S2 from S1 be delivered after the T1 is up again? If so, in both cases?

Q31. P17: What about PDU's that are at large as the MTU? May PDU2 be larger than the MTU or must it split into two packets?

Q32. P18: What are the criteria for negotiation on other media for delivering H1. Will negotiation take place on individual bases or for all ISP's and LEA's together?

Q33. P14: For T1 – T 2 communications a physically secured and total administrative control is a secure channel. Does this also count for S1 – S2?
More generally: What are secure channels?

Q34. P18: Must S2 deliver the traffic to at most 5 T1's? What is the purpose of this?
Can the use of several T1's be explained, because it is not quite clear in the document?
One possibility is to deliver to more than one T1. The other is to have different routes for delivering to the LEA.

Q35. P20: Here it seems that S1 has warrants. The warrants should be set up on S2 and not S1, is this correct? S2 set up the tunnel. Why and how does S1 have to torn it down?

Q36. P20: Isn't it true that there is only one warrant per tunnel? So the tunnel should always be torn down after the warrant ends?

Q37. P20: Can the use of target location be explained? Who gives the X and Y coordinates and how are the established?

Q38. P20/21: Must DHCP renewal events given to T1? If so, is it via SuccessfulIPv4DHCPRegistration?

Q39. P20: Is there a fixed format for the telephone number?

Q40. How must S2 authenticate S1? Is it up to the ISP?

Q41. P23: In chapter 12.1 more functionality is given to both HI1 as HI2. Why not in the specific chapters?

Q42. P23: How must S2 handover a log event when there is no session established?

Q43. P23: In the previous chapters it seems that HI1 is a one way channel from LEA to ISP. Is it true that log events could go over HI1? So, it would be bi-directional. What is the procedure in this case? How is the data transferred and in which format? Consider the fact that HI1 will be electronic in the future, without human interference.

Q44. P24: It is stated that randomly a given tunnel should be used. Can this be clarified?
In the specifications it seems that there is only one tunnel per warrant. See also Question 34.

Q45. P26. Who gives the X.509 certificates?

Q46. P26. Is it true that a specific X.509 certificate can be used for more than 1 warrant?
This seems to be the fact, since it is stated that a certificate expires after one year.

Q47. Why are the terms SSLv3 and TLS both mentioned all the ways? Can this be clarified?

Q.48. P6: Is it correct that events (authentication, log) are transmitted from S2 to T1 after they are received by the server and not during the event itself?

Q49. Chapter 9 en 12. It is not clearly specified howHI3: Email packet in IP PDU is build. What is the payload of a Email Packet in an IP PDU? Are the IP packets of SMTP communication of E-mail addressed (TO,CC en BCC) to the target or is it the email text message as specificied in RFC 822 en RFC 821?

Q50. TIIT v0.1.2 12.2 Message formats of intercepted traffic: de specification of a IP PDU for intercepted email (conform RFC 822) is forgotten. Is this true?