LAMPIRAN
PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA
NOMOR 8 TAHUN 2014
TENTANG
PERSYARATAN TEKNIS ALAT DAN PERANGKAT PENYADAPAN YANG SAH ATAS INFORMASI BERBASIS *INTERNET PROTOCOL* PADA PENYELENGGARAAN JARINGAN BERGERAK SELULER DAN JARINGAN TETAP LOKAL TANPA KABEL DENGAN MOBILITAS TERBATAS

PERSYARATAN TEKNIS ALAT DAN PERANGKAT PENYADAPAN YANG SAH ATAS INFORMASI BERBASIS *INTERNET PROTOCOL* PADAPENYELENGGARAAN JARINGAN BERGERAK SELULER DAN JARINGAN TETAP LOKAL TANPA KABEL DENGAN MOBILITAS TERBATAS

Ruang lingkup Peraturan Menteri ini meliputi:

1. BAB I : Ketentuan Umum;
2. BAB II : Persyaratan *Handover Interface* untuk Layanan Pengiriman *Internet Protocol;*
3. BAB III : Sertifikasi;

BAB I
KETENTUAN UMUM

1. Dalam Peraturan Menteri ini yang dimaksud dengan :

   1.1. *Handover Interface* yang selanjutnya disingkat HI adalah antarmuka fisik dan virtual tempat di mana langkah-langkah penyadapan diminta dari penyelenggara jaringan telekomunikasi bergerak seluler serta penyelenggara jaringan tetap lokal tanpa kabel dengan mobilitas terbatas (*fixed wireless access)* dan hasil penyadapannya dikirimkan dari penyelenggara jaringan telekomunikasi bergerak seluler serta penyelenggara jaringan tetap lokal tanpa kabel dengan

mobilitas terbatas *(fixed wireless access)* kepada fasilitas monitoring penegak hukum.

1.2. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.

1.3. Penyadapan yang sah (*lawful interception*) atas informasi adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi yang dilaksanakan oleh aparat penegak hukum dan/atau badan intelijen yang berwenang berdasarkan ketentuan peraturan perundang-undangan.

1.4. Antarmuka penyadapan adalah lokasi fisik atau virtual dalam fasilitas telekomunikasi milik penyelenggara jaringan/penyelenggara jasa/penyedia akses dimana tersedia akses ke isi komunikasi dan informasi terkait penyadapan.

1.5. Informasi terkait penyadapan (*Intercept Related Information*)yang selanjutnya disingkat IRI adalah kumpulan informasi atau data terkait dengan layanan telekomunikasi yang melibatkan identitas target, informasi atau data yang terkait komunikasi khusus termasuk upaya komunikasi yang tidak berhasil, layanan yang terkait informasi atau data misalnya manajemen profil layanan oleh pelanggan, dan informasi lokasi.

1.6. Fungsi penyadapan internal (*Internal InterceptionFunction*) yang selanjutnya disingkat IIF adalah titik dalam suatu jaringan atau unsur jaringan di mana isi komunikasi dan informasi terkait penyadapan tersedia.

1.7. Antarmuka jaringan internal (*Internal Network Interface*) yang selanjutnya disingkat INI adalah antarmuka internal milik jaringan antara IIF dan fungsi mediasi.

1.8. Aparat Penegak Hukum yang selanjutnya disingkat APH adalah organisasi yang berwenang untuk meminta upaya penyadapan dan menerima hasil penyadapan telekomunikasi dalam rangka penegakan hukum.

1.9. Lembaga Intelijen Negara yang selanjutnya disingkat LIN adalah organisasi yang berwenang untuk meminta penyadapan dan menerima hasil penyadapan telekomunikasi dalam rangka keamanan nasional.

1.10. Fasilitas monitoring penegak hukum (*Law Enforcement Monitoring Facility*) yang selanjutnya disingkat LEMF adalah fasilitas yang dirancang sebagai tujuan transmisi hasil penyadapan terkait dengan subjek penyadapan tertentu baik yang ditempatkan di APH maupun di LIN.

1.11. Fungsi mediasi (*Mediation Function*) yang selanjutnya disingkat MF adalah mekanisme yang melewatkan informasi antra suatu penyelenggara jaringan, penyelenggara jasa atau penyedia akses dan suatu HI, dan informasi antara INI dan HI.

1.12. Penyelenggaraan jaringan telekomunikasi adalah kegiatan penyediaan dan atau pelayanan jaringan telekomunikasi yang memungkinkan terselenggaranya telekomunikasi.

1.13. Penyelenggaraan jasa telekomunikasi adalah kegiatan penyediaan dan atau pelayanan jasa telekomunikasi yang memungkinkan terselenggaranya telekomunikasi.

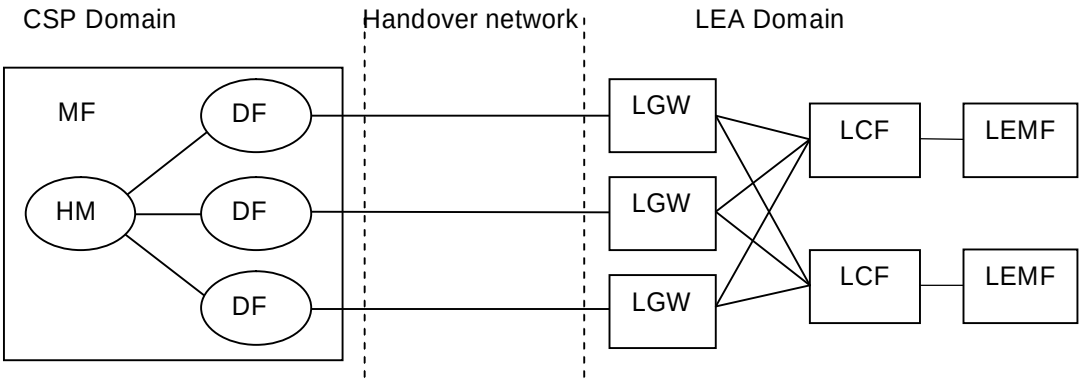
1.14. Telekomunikasi adalah setiap pemancaran, pengiriman, dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik Iainnya.

2. Lingkup Persyaratan Teknis

Peraturan ini menjelaskan penerapan ETSI TS 102 232 di Indonesia, dengan lingkup pengaturan persyaratan *Handover Interface* dan Layanan untuk pengiriman *internet protocol* termasuk:

a. *Handover specification for* IP *delivery;*
b. *Service-specific details for E-mail services;*
c. *Service-specific details for internet access services;*
d. *Service-specific details for Layer* 2 *services;*
e. *Service-specific details for* IP *Multimedia services;*
f. *Service-specific details for* PSTN/ISDN *services.*
g. *Service-specific details for Mobile services.*

3. Konfigurasi



konfigurasi LEMF Gateway pada sisi LEA/APH di Indonesia

3.1. Penjelasan dari konfigurasi pada gambar di atas yaitu:

a. *Handover Manager* (HM) bertugas untuk melakukan handover data yang disadap dari seluruh penyadapan yang berjalan kepada tujuan-tujuan yang sesuai. Untuk melakukan hal tersebut, *Handover Manager* membuat paling sedikit satu *Delivery Function* (DF) (lihat ETSI TS 102 232-1 klausul 6.3).

b. Untuk alasan fungsional mengenai ketersediaan, *multi Delivery Functions* dapat dibuat masing-masing mengarah kepada tujuan antara yang berbeda, sebuah unsur yang disebut *LEMF-Gateway* (LGW).

c. Hanya satu jalur komunikasi virtual satu arah dari DF ke LGW yang diperbolehkan.

d. MF *Handover Manager* bertanggung jawab untuk pendistribusian PDU pada *LEMF-Gateway* yang sesuai.

e. *LEMF-Collection Function* (LCF) bertanggung jawab untuk mengumpulkan trafik dari LGW dan pengiriman ke LEMF.

3.2. Handover *Manager* (HM)

Handover Manager melaksanakan kegiatan sebagai berikut:

a. Mengagregasi atau memisah-misahkan *payloads* jika diperlukan (lihat ETSI TS 102 232-1 klausul 6.2.3 dan 6.2.4);

b. Mengumpulkan informasi header (lihat ETSI TS 102 232-1 klausul 5.2);

c. Membuat *padding PDUs* jika diperlukan (lihat ETSI TS 102 232-1 klausul 6.2.5);

d. Mengalokasikan PDUs ke suatu *Delivery Function* (lihat ETSI TS 102 232-1 klausul 6.2.1).

e. Kecuali untuk tujuan *debugging*, seluruh PDU dienkripsi dengan suatu kunci kriptografi yang diketahui. Kunci ini ditetapkan untuk masing-masing LIID dalam HI1.

3.3. *Delivery Function* (DF)

Delivery Function bertanggung jawab untuk operasi berikut:

a. DF membuka, membuat dan memelihara suatu TLS *tunnel* ke setiap LGW yang ditetapkan dalam autorisasi legal. Kunci-kuncinya dinegosiasikan melalui HI1. Jika suatu LGW tidak dapat dicapai maka DF mencoba untuk menyambung kembali.

b. TLS *tunnel* hanya menerima penggunaan *cryptosuites* yang dibolehkan. Ketentuan ini diambil karena negosiasi dari *cryptosuites* selain dari yang dibolehkan mengakibatkan terputusnya sambungan (diskoneksi) *tunnel*. Dalam hal ini suatu alarm dapat digunakan untuk personel berwenang.

c. DF membuka, membuat dan memelihara suatu TLS *tunnel* ke setiap LGW dengan menggunakan TCP-port 3004.

3.4. *LEMF-Gateway* (LGW)

LEMF-Gateway melakukan operasi berikut:

a. LGW menerima TLS *tunnel* yang datang dari setiap unit fungsional DF yang diketahui. Diketahui artinya bahwa kedua alamat IP dan *public key* dari DF tersedia untuk LGW. Kunci-kunci tersebut dinegosiasikan melalui HI1.

b. LGW menerima trafik dari setiap unsur fungsional DF yang mana ia mempunyai suatu hubungan *client-server* terautentikasi. Trafik yang diterima akan diteruskan ke suatu fungsi pengumpulan LCF. LCF mana yang akan dipilih tergantung kepada *Lawful Interception Identifier* (LIID) dan kepada informasi jenis *Payload* terenkripsi dalam *Header* terenkripsi dari PDU.

c. LGW dapat mengirimkan paket-paket yang datang ke lebih dari satu LCF.

d. LGW mendengarkan koneksi layanan berbasis TLS yang datang pada TCP-port 3004.

e. LGW dapat mem-*buffer* PDU (lihat ETSI TS 102 232-1 klausul 6.3.3).

3.5. *LEMF-Collection Function* (LCF)

LCF merupakan bagian dari LEMF. LCF melakukan operasi sebagai berikut:

a. LCF hanya menerima TLS *tunnel* yang datang dari LEMF-Gateway yang diketahui.

b. LCF mendengarkan koneksi layanan berbasis TLS yang datang pada TCP-port 3004.

c. LCF men-dekripsi seluruh PDU dengan kunci kriptografik yang dinegosiasikan melalui HI1.

d. LCF dapat mem-*buffer* PDU yang di-enkripsi atau di-dekripsi.

e. LCF mengirimkan PDU yang di-dekripsi ke LEMF melalui TCP-port 3003.

3.6. *LEMF*

LEMF menerima koneksi yang datang dari LCF melalui TCP-port 3003.

4. Singkatan

ASN.1	: *Abstract Syntax Notation One*
CC	: *Content of Communication*
CIN	: *Communication Identity Number*
DCC	: *Delivery Country Code*
DF	: *Delivery Function*
ETSI	: *The European Telecommunications Standards Institute*
HI1	: *Handover Interface 1 (for Administrative Information)*
HI2	: *Handover Interface 2 (for Intercept Related Information)*
HI3	: *Handover Interface 3 (for Content of Communication)*
IRI	: *Intercept Related Information*
LEA/APH	: *Law Enforcement Agency*/Aparat Penegak Hukum
LEMF	: *Law Enforcement Monitoring Facility*
LGW	: *Local Gateway*
LIID	: *Lawful Interception IDentifier*
MF	: *Mediation Function*
NEID	: *Network Element IDentifier*
NID	: *Network Identifier*
PDU	: *Protocol Data Unit*

PS	: *Packet Switched*
PJBS	: Penyelenggara Jaringan Bergerak Seluler
PJFWA	: Penyelenggara Jaringan Tetap Lokal Tanpa Kabel dengan Mobilitas Terbatas
RTP	: *Real Time Protocol*
SSD	: *Service-Specific Details*
TCP	: *Transmission Control Protocol*
TLS	: *Transport Layer Security*
UDP	: *User Datagram Protocol*
LIN	: Lembaga Intelijen Negara

5. Rujukan

5.1. ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery " versi 3.1.1 (2012-06).

5.2. ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-Specific Details for E-mail services" version 3.2.1 (2012-06).

5.3. ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-Specific Details for internet access services" version 3.2.1 (2012-06).

5.4. ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-Specific Details for Layer 2 services" version 3.1.1 (2012-02).

5.5. ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-Specific Details for IP Multimedia Services" version 3.2.1 (2012-06).

5.6. ETSI TS 102 232-6: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-Specific Details for PSTN/ISDN services" version 3.1.1 (2012-06).

5.7. ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-Specific Details for Mobile services" version 3.1.1 (2012-06).

5.8. ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic" version 3.10.1 (2012-06).

5.9. ITU-T Recommendation G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".

5.10. IETF RFC 0793: “Transmission Control Protocol (TCP)”.

5.11. IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

5.12. IETF RFC 5246: "*The Transport Layer Security (TLS) Protocol Version 1.2*".

6. Nomor-nomor versi dari dokumen-dokumen terkait.

Tabel ini dicantumkan untuk tujuan pemeliharaan yang memberikan suatu ringkasan mengenai versi-versi dari dokumen-dokumen rujukan normatif yang digunakan selama implementasi dari peraturan ini. Daftar spesifikasi rujukan dengan nomor-nomor versinya:

Bagian TS 102 232:	N/I	Dokumen rujukan normatif dalam bagian-bagian ETSI TS 102 232	Versi s.d. 15-08-2011
5	N	ATIS-PP-1000678.2006: "Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunication Networks", Version 2 (Revision of ANS T1.678-2004).	2006
1	I	ETSI ES 201 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".	1.2.1 (2002-04)
6	I	ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".	1.1.1 (2006-03)
1	I	ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".	ed.1 (1995-11)
1,2,4,5	I	ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".	1.3.1 (2009-10)
1,2,3,4,5,6,7	N	ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".	3.8.1 (2011-08)
1	N	ETSI TS 101 909-20-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services".	1.1.2 (2005-10)
1	N	ETSI TS 101 909-20-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services".	1.2.1 (2006-03)
2,3,4,5,6,7	N	ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover	2.7.1 (2011-08)

		specification for IP delivery".	
1,4	N	ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for E-mail services".	2.6.1 (2011-08)
1,4	N	ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".	2.3.1 (2011-08)
1	N	ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".	2.3.1 (2010-08)
1	N	ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".	2.5.1 (2010-10)
1	N	ETSI TS 102 232-6: "Lawful interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".	2.3.1 (2008-08)
1	N	ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".	2.2.1 (2011-03)
4		ETSI TS 123 060: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2 (3GPP TS 23.060 Release 6)".	10.4.0 (2011-06)
1,2,5,7	N	ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 Release 9)".	10.4.0 (2011-06) 9.6.0 (2011-04) 8.13.0 (2011-04) 7.10.0 (2011-02)
6	I	ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Lawful interception functional entities, information flow and reference points".	2.1.1 (2009-09)
1		FIPS PUB 186-2: "Digital Signature Standard (DSS)".	27 Januari 2000
3		IEEE 802.11 (ISO/IEC 8802-11): "IEEE Standards for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan AreaNetwork - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".	2007

1		IETF RFC 0791: "Internet Protocol".	September 1981
1		IETF RFC 0792: "Internet Control Message Protocol".	September 1981
1	N	IETF RFC 0793: "Transmission Control Protocol".	September 1981
1,3,4		IETF RFC 1122: "Requirements for Internet Hosts – Communication Layers".	Oktober 1989
1		IETF RFC 1191: "Path MTU discovery".	November 1990
1		IETF RFC 1323: "TCP Extensions for High Performance".	Mei 1992
3,4		IETF RFC 1570: "PPP LCP Extensions".	Januari 1994
4		IETF RFC 1661: "The Point-to-Point Protocol (PPP)".	Juli 1994
2		IETF RFC 1939: "Post Office Protocol - Version 3".	Mei 1996
3		IETF RFC 1990: "The PPP Multilink Protocol (MP)".	Agustus 1996
1		IETF RFC 2018: "TCP Selective Acknowledgement Options".	Oktober 1996
3		IETF RFC 2131: "Dynamic Host Configuration Protocol".	Maret 1997
3	N	IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".	Maret 1997
4		IETF RFC 2341: "Cisco Layer Two Forwarding (Protocol) L2F".	Mei 1998
4	N	IETF RFC 2427: "Multiprotocol Interconnect over Frame Relay".	September 1998
1		IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".	Desember 1998
2		IETF RFC 2595: "Using TLS with IMAP, POP3 and ACAP".	Juni 1999
4		IETF RFC 2637: "Point-to-Point Tunneling Protocol (PPTP)".	Juli1999
4		IETF RFC 2661: "Layer Two Tunneling Protocol (L2TP)".	Agustus 1999
4	N	IETF RFC 2684: "Multiprotocol Encapsulation over ATM Adaptation Layer 5".	September 1999
3		IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".	Juni 2000
3		IETF RFC 2866: "RADIUS Accounting".	Juni 2000
1		IETF RFC 2923: "TCP Problems with Path MTU Discovery".	September 2000
3,4		IETF RFC 3046: "DHCP Relay Agent Information Option".	Januari 2001
3		IETF RFC 3118: "Authentication for DHCP Messages".	Juni 2001

1		IETF RFC 3174: "US Secure Hash Algorithm 1 (SHA1)".	September 2001
2		IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security".	Februari 2002
5		IETF RFC 3261: "SIP: Session Initiation Protocol".	Juni 2002
3		IETF RFC 3396: "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)".	November 2002
2		IETF RFC 3493: "Basic Socket Interface Extensions for IPv6".	Februari 2003
2		IETF RFC 3501: "Internet Message Access Protocol - Version 4 rev1".	Maret 2003
5	N	IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".	Juli 2003
6	N	IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control".	Juli 2003
3		IETF RFC 4282: "The Network Access Identifier".	Desember 2005
2		IETF RFC 4422: "Simple Authentication and Security Layer (SASL)".	Juni 2006
5,6	N	IETF RFC 4566: "SDP: Session Description Protocol".	Juli 2006
2		IETF RFC 4616: "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism".	Agustus 2006
2		IETF RFC 4954: "SMTP Service Extension for Authentication".	Juli 2007
5		IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".	September 2007
1	N	IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".	Agustus 2008
1		IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile",	Mei 2008
1,2		IETF RFC 5321: "Simple Mail Transfer Protocol".	Oktober 2008
1,2		IETF RFC 5322: "Internet Message Format".	Oktober 2008
1		IETF RFC 5681: "TCP Congestion Control".	September 2009
1		IETF RFC 6298: "Computing TCP's Retransmission Timer".	Juni 2011
1,2,3	N	ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".	Juli 2007
1		ISO/IEC TR 10000-1: "Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General	Oktober 1998

		principles and documentation framework".	
4		ITU-T Recommendation E.164: "The international public telecommunication numbering plan".	November 2010
6	N	ITU-T Recommendation G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".	November 1988
5		ITU-T Recommendation H.225.0: "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".	Desember 2009
5		ITU-T Recommendation H.245: "Control protocol for multimedia communication".	Mei 2011
5		ITU-T Recommendation H.248: "Gateway control protocol". NOTE: H.248 was renumbered when revised on 2002-03-29. H.248 main body, Annexes A to E and Appendix I were included in H.248.1. Subsequent annexes were sequentially numbered in the series, e.g. H.248 Annex F became H.248.2	
5		ITU-T Recommendation H.323: "Packet-based multimedia communications systems".	Desember 2009
2		ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".	November 1988
1,2,3,4,5,6		ITU-T Recommendation X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".	November 2008
1		ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".	November 2008
1,7	I	TIA/ATIS ANSI/J-STD-025-B: "Lawful Authorized Electronic Surveillance," (August 2006) as amended by ANSI/J-STD-025-B-1 "Lawfully Authorized Electronic Surveillance (LAES) Addendum 1–Addition of Mobile Equipment IDentifier (MEID)" (September 2006) and by ANSI/J-STD-025-B-2 "Lawfully Authorized Electronic Surveillance (LAES) – Addendum 2 - Support for Carrier Identity" (April 2007).	Agustus 2006
7	I	US 103rd Congress, Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, 108 STAT. 4279 (Oct. 25, 1994).	Oktober 1994
CATATAN:	N=Normatif, I=Informatif Spesifikasi diindikasikan sebagai Normatif: 1) dalam hal ASN.1 merupakan data yang diimpor dari spesifikasi		

	tersebut; 2) spesifikasi dirujuk dalam definisi ASN.1; 3) spesifikasi dirujuk dalam persyaratan teknis ini.

BAB II

PERSYARATAN HANDOVER INTERFACE UNTUK LAYANAN PENGIRIMAN *INTERNET PROTOCOL*

1. Umum

Rujukan: ETSI TS 102 232-1 klausul 4

2. Headers

Rujukan: ETSI TS 102 232-1 klausul 5

2.1. Lawful Interception IDentifier *(ETSI TS 102 232-1 klausul 5.2.2)*

a. Untuk setiap permintaan penyadapan harus ditetapkan suatu *identifier* yang secara global unik. Hal ini bisa dicapai dengan menggunakan *Lawful Interception IDentifier* (LIID) yang terdiri dari 8 digit desimal yang diikuti oleh suatu *MD5 hash*, dua oktet untuk penggunaan oleh PJBS dan PJFWAdan tiga oktet untuk penggunaan pada masa yang akan datang. LIID ditetapkan oleh APH dan LIN.

b. Panjang keseluruhan dari LIID adalah 25 oktet:
   1) 8 digit desimal (BCD encoded, 4 oktet);
   2) *MD5 hash* (16 oktet);
   3) Untuk penggunaan PJBS (nilai default 0xFF00 ditetapkan oleh APH atau LIN, 2 oktet);
   4) Dicadangkan untuk penggunaan di masa yang akan datang (nilai awal 0xFF00FF, 3 oktet).

c. Contoh LIID:
   12345678001122334455667788 99AABBCCDDEEFFFF00FF00FF

d. Dengan cara ini APH atau LIN dapat mengeluarkan*identifier*-nya sendiri, tidak tergantung kepada *Law Enforcement Monitoring Facility* (LEMF) jika paket data akan disadap.

e. APH atau LIN dapat mengabaikan lima oktet terakhir saat *identifier* diterima melalui HI2 dan/atau HI3.

2.2. Kode negara otorisasi *(ETSI TS 102 232-1klausul 5.2.3)*
Kode negara otorisasi untuk permintaan penyadapan yang berasal dari Indonesia: ID

2.3. *Communication identifier (ETSI TS 102 232-1 klausul 5.2.4)*

a. *Network Identifier* (NID) terdiri dari *operator identifier* dan *Network Element IDentifier* (NEID). NEID harus dilaksanakan dan digunakan seperti ditetapkan dalam TS 101 671. *Operator identifier* harus terdiri dari 8 karakter desimal yang secara internasional unik menggambarkan suatu operator jaringan, penyedia akses atau penyedia jasa dan bersifat wajib sesuai dengan ketentuan *Fundamental Technical Plan* (FTP).

b. Penggunaan ekstensi CIN didukung.

c. *Delivery country code* (DCC) untuk Indonesia adalah: ID.

2.4. *Payload timestamp (ETSI TS 102 232-1 klausul 5.2.6)*

a. Penggunaan *MicroSecondTimeStamp* bersifat wajib untuk HI1, HI2 dan HI3 untuk seluruh layanan/jasa.

b. Penggunaan *timeStampQualifier field* bersifat wajib untuk seluruh layanan/jasa.

2.5. Arah *payload (ETSI TS 102 232-1 klausul 5.2.7)*

Penggunaan arah dari *payload* bersifat wajib.

2.6. Jenis IRI *(ETSI TS 102 232-1 klausul 5.2.10)*

Penggunaan jenis IRI bersifat wajib.

---

3. Pertukaran data

Rujukan: ETSI TS 102 232-1 klausul 6

3.1. Lapisan *handover*, umum *(ETSI TS 102 232-1 klausul 6.2.1)*

a. PDU harus didistribusikan secara acak kepada seluruh DF yang tersedia.

b. Jalur komunikasi virtual adalah satu arah, yaitu dari DF ke LGW.

3.2. Pelaporan *error (ETSI TS 102 232-1klausul 6.2.2)*
Pelaporan *error* dari MF *Handover Manager* ke LEMF *Handover Manager* tunduk kepada perjanjian kerja sama antara PJBS/PJFWA dan APH/LIN.

3.3. Aggregasi *payload (ETSI TS 102 232-1 klausul 6.2.3)*

a. Aggregasi *payload* harus dilakukan menurut klausul 6.2.3dalam ETSI TS 102 232-1.
b. Pada satu detik atau satu Megabyte pertama dari trafik, *Payload CC* (yang diukur pada *payload* yang disadap) dapat diagregasikan dalam satu PS-PDU. Timestamp pada masing-masing (yaitu *payload CC*) harus disediakan. *Payload* IRI dapat diagregasikan.

3.4. Pengiriman sekumpulan besar data level aplikasi *(ETSI TS 102 232-1 klausul 6.2.4)*
Data level aplikasi harus disegmentasi saat melebihi ukuran 1 (satu) Megabyte.

3.5. Padding *data (ETSI TS 102 232-1 klausul 6.2.5)*
Pengiriman padding data melalui *handover interface* dibolehkan berdasarkan perjanjian kerjasama.

3.6. *Payload encryption (ETSI TS 102 232-1 klausul 6.2.6)*

a. *Delivery manager* harus melakukan *handover* terenkripsi dengan menggunakan *Payload* terenkripsi struktur ASN.1. Jenis enkripsi dapat berupa AES-192-CBC, AES-256-CBC, Blowfish-192-CBC, Blowfish-256-CBC, dan Threedes-CBC.
b. Penggunaan jenis *payload* terenkripsi adalah wajib.

3.7. *Session layer*, umum *(ETSI TS 102 232-1 klausul 6.3.1)*
Jalur dari DF ke LEMF harus merupakan suatu *tunnel* terenkripsi menurut TLS RFC 5246. Penggunaan *plain TCP* (IETF RFC 0793) dibolehkan hanya untuk tujuan *debugging*.

3.8. *Pembukaan* dan penutupan koneksi *(ETSI TS 102 232-1 klausul 6.3.2)*
Interval percobaan kembali upaya koneksi harus dapat dikonfigurasikan antara 30 dan 300 detik. Interval default adalah 30 detik.

3.9. Buffering *(ETSI TS 102 232-1 klausul 6.3.3)*
Ukuran dari *cyclic buffer* harus cukup untuk menampung (*buffering*) sejumlah trafik yang mencakup interval percobaan kembali yang aktual seperti didefinisikan dalam klausul 4.8 ditambah 5 detik dengan sebanyak-banyaknya setengah dari RAM.

3.10. *Keep alives (ETSI TS 102 232-1 klausul 6.3.4)*
Session Layer "*keep alives*" wajib digunakan.

3.11. Lapisan *transport*, TCP settings *(ETSI TS 102 232-1 klausul 6.4.2)*

a. Nomor port untuk TLS adalah 3004.
b. Nomor port untuk plain TCP adalah 3003.

3.12. Pemberitahuan data *(ETSI TS 102 232-1 klausul 6.4.3)*
Data dianggap berhasil terkirim saat pemberitahuan TCP telah diterima.

---

4. Jaringan pengiriman

Rujukan: ETSI TS 102 232-1 klausul 7

4.1. Jenis jaringan, umum *(ETSI TS 102 232-1 klausul 7.1)*
Jaringan yang digunakan untuk pertukaran data dibatasi untuk *leased line* atau *private network* untuk layanan telekomunikasi bergerak seluler.

4.2. Persyaratan keamanan, umum *(ETSI TS 102 232-1 klausul 7.2.1)*
Jalur dari DF ke LGW harus merupakan *tunnel* terenkripsi menurut TLS RFC 5246.

4.3. Kerahasiaan dan autentikasi *(ETSI TS 102 232-1 klausul 7.2.2)*

Enkripsi harus didasarkan pada TLS_RSA_WITH_RC4_128_SHA atau LS_DHE_RSA_WITH_AES_256_CBC_SHA RFC 5246.

4.4. Integritas *(ETSI TS 102 232-1 klausul 7.2.3)*

a. Memasukkan "*message digests*" menggunakan SHA-1 (melihat acuan RFC 3174) adalah wajib, tidak tergantung pada antarmuka HI1.
b. Nilai default berikut harus dapat dikonfigurasikan sesuai dengan ETSI TS 102 232-1klausul 7.2.3. Nilai default saat ini adalah:
<*trafficTime*>:1 (satu) detik
<pduCount>:tidak digunakan
<hashTimeout>:300 detik
<*predefined number of*> *IntegrityCheck PDUs:* 15

<*predefined number of*> *seconds:*1800

4.5. Data uji *(ETSI TS 102 232-1 klausul 7.3.1)*
Pembangkitan PDU uji secara otomatis pada aktivasi penyadapan tidak digunakan.

5. Rincian Spesifik Layanan (*Service Specific Details*)

5.1. Persyaratan untuk Layanan E-mail (*ETSI TS 102 232-2*)

a. SMTP HI2 event-record mapping

Rujukan: ETSI TS 102 232-2 klausul A.4 Tabel A2: SMTP E-mail event records

SMTP events	Subject	HI2 record
E-mail send successful	Client	Report
E-mail send unsuccessful	Client	Report

b. POP3 HI2 event-record mapping

Rujukan: ETSI TS 102 232-2 klausul B.4 Tabel B.2: POP3 E-mail event records

POP3 events	Subject	HI2 record
E-mail download	Client	Report
E mail partial download	Client	Report

c. Indikasi Validitas Pengirim e-mail
Rujukan: ETSI TS 102 232-2 klausul F.2: SMTP protocol characteristics.
Penggunaan "e-mail-*Sender-Validity*" untuk menunjukkan jaminan oleh PJBS mengenai alamat e-mail adalah wajib.

5.2. Persyaratan untuk Layanan Akses Internet (*ETSI TS 102 232-3*)
Atribut HI2

Rujukan: ETSI TS 102 232-3 klausul 6.2

5.3. Persyaratan untuk Layanan Layer 2 (*ETSI TS 102 232-4*)

a. IRI Event

Rujukan: ETSI TS 102 232-4 klausul 6.1
Alokasi CIN harus dilakukan pada *Access Attempt.*

b. Lokasi Target
Rujukan: ETSI TS 102 232-4 klausul 8.1 (L2IRIContents) dan klausul A.1.1 tabel A.1 sampai tabel A.8
Lokasi target tidak diperlukan selama masih dalam kajian oleh ETSI.

5.4. Persyaratan untuk Layanan IP Multimedia (*ETSI TS 102 232-5*)

a. Persyaratan Umum
Rujukan: ETSI TS 102 232-5 klausul 4.3
Item 6) tidak berlaku. *Mapping* informasi IRI ke dalam pesan-pesan pada handover interface tidak digunakan.

b. Jenis event dan rekaman IRI
Rujukan: ETSI TS 102 232-5 klausul 5.4
Penggunaan jenis rekaman IRI BEGIN, CONTINUE dan END tidak diwajibkan. Jika jenis Rekaman IRI tidak dibedakan, jenis Rekaman IRI adalah REPORT.
Pemilihan implementasinya (BEGIN-CONTINU-END atau REPORT) dilakuan per sesi komunikasi.

c. Penyadapan dan Isi Komunikasi (*Content of Communication*)
Rujukan: ETSI TS 102 232-5 klausul 5.5
RTP CC harus selalu mengandung RTP *header*. Jika RTP *header* tidak tersedia, CSP harus menambahkan suatu *header* valid artifisial sesuai dengan RFC 3550.
RTP CC harus mengandung UDP *header* dan IP *header* jika tersedia.

d. Korelasi IRI dan CC
Rujukan: ETSI TS 102 232-5 klausul 6.2
Dalam hal *multiple media streams*, penggunaan *streamIdentifier field* untuk suatu korelasi tambahan adalah dibolehkan.

e. Jumlah minimum atribut fungsional yang harus disediakan
Rujukan: ETSI TS 102 232-5 annex B
Jumlah minimum dari atribut fungsional didefinisikan dalam annex B. Item spesifik ditetapkan dalam persyaratan teknis ini (misal seperti *buffering* dalam bagian 3.9).

5.5. Persyaratan untuk Layanan PSTN/ISDN (ETSI TS 102 232-6)

a. Format CC
Rujukan: ETSI TS 102 232-6 klausul 6.2
Jika tidak ada indikasi *codec* sama sekali maka *codec default* yang dikirim adalah G.711.

b. Pengiriman informasi tambahan
Rujukan: ETSI TS 102 232-6 klausul 6.3.3
Informasi tambahan harus dikirimkan sabagai IRI. Bila *codec* bukan G.711 maka informasi tambahan harus juga dikirimkan sebagai CC-PDUs (dalam hal ini sedikitnya dalam PDU pertama dan dalam PDU-PDU berikutnya hanya jika ada perubahan selama sesi ini).

c. Fungsionalitas LI
Fungsionalitas layanan PSTN/ISDN yang dikirim dijelaskan dalam ETSI TS 101 671.

5.6. Persyaratan untuk Layanan Bergerak (*Mobile Services)*
Seluruhnya merujuk *ETSI TS 102 232-7*.

BAB III
SERTIFIKASI

Sertifikasi alat dan perangkat untuk penyadapan yang sah atas informasi yang berbasis *internet protocol* pada penyelenggaraan jaringan bergerak seluler dan jaringan tetap lokal tanpa kabel dengan mobilitas terbatas dilaksanakan sesuai peraturan perundang-undangan.

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA,

TIFATUL SEMBIRING