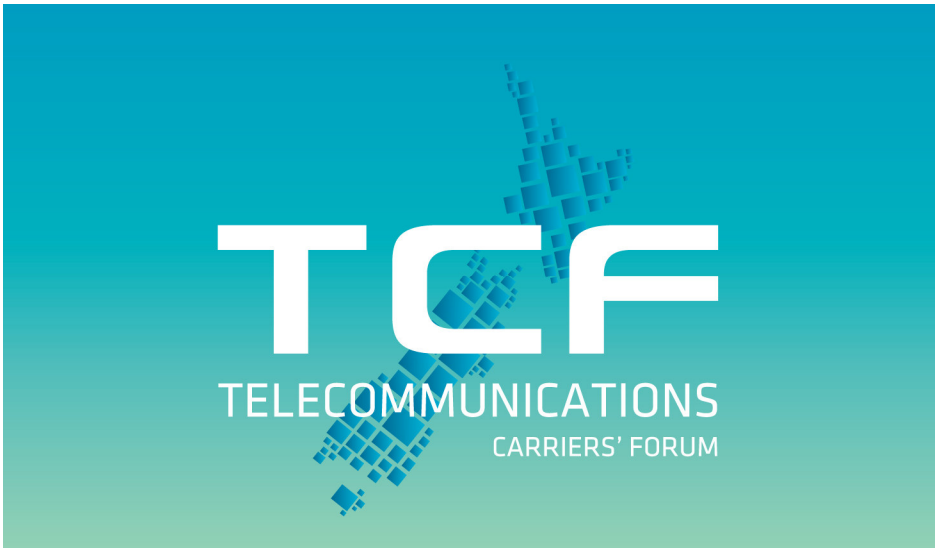


Guidelines for Interception Capability

August 2009

CONTENTS

A. FOREWORD

1. Network Operators and Service Providers in New Zealand are obligated to ensure that public Telecommunications networks and Telecommunications Services have Interception Capability in compliance with the Telecommunications (Interception Capability) Act 2004 (TICA).

   This obligation became due for the Public Switched Telephone Network (PSTN) 18 months from the commencement of the TICA (15 October 2005) and the Public Data Network (PDN) was due five years after that date (5 April 2009).

   Network Operators and Service Providers in New Zealand have worked with Law Enforcement Agencies to meet these obligations - initially with PSTN compliance, and latterly towards meeting PDN compliance.

   It has become apparent both from overseas experience, and the work done so far in New Zealand, that a set of industry guidelines regarding the adoption of standards, architectures and processes would greatly benefit existing Network Operators, Service Providers and new entrants to achieve compliance with the TICA.

   The benefits, in terms of operational cost savings, would extend to the Law Enforcement Agencies as well as the Network Operators and Service Providers as a result of streamlining the compliance process, by clarifying the requirements for both the solution architectures and interfaces.

   As a summary, these guidelines provide:

   1.1. An interpretation of the TICA with regards to the Network Operators and Service Providers obligations, as outlined therein.
   1.2. Relevant standards.
   1.3. Overall solution architectures.
   1.4. Mediation (dedicated and hosted).
   1.5. Interception technology -
      1.5.1 internal intercept functions;
      1.5.2 external intercept functions;
      1.5.3 tactical solutions; and
      1.5.4 security requirements.
   1.6. Agency technology -
      1.6.1 call data interfaces; and
      1.6.2 call content interfaces.

B. PURPOSE

2. The purpose of these guidelines is to provide assistance to Network Operators and Service Providers in New Zealand to comply with the TICA in an efficient, timely and cost effective manner.

3. These guidelines must be read in conjunction with the TICA; the TICA takes precedence over these guidelines.

4. Meeting these guidelines will materially assist in achieving compliance with the requirements of the TICA.

5. The TICA has specific obligations on both Network Operators and Service Providers. Under the terms of the TICA, only Network Operators are required to have an

Interception Capability. However, it can be expected that most TCF members would fall into the Network Operator category.

6. Where there is any ambiguity between these guidelines and the TICA, Network Operators and Service Providers should consult their own independent legal advice and consult with the Surveillance Agencies through the Lawful Interception administrator (the "Administrator").

7. These guidelines will take effect from the date they are endorsed by the TCF.

C. DEFINED TERMS

In these guidelines, unless the context otherwise requires:

"Act" means the Telecommunications (Interception Capability) Act 2004 (TICA).

"Call Associated Data (CAD)" has the same definition as in the TICA, which means call associated data in relation to a Telecommunication —

(a) means information —
  (i) that is generated as a result of the making of the Telecommunication (whether or not the Telecommunication is sent or received successfully); and
  (ii) that identifies the origin, direction, destination, or termination of the Telecommunication; and
(b) includes, without limitation, any of the following information -
  (i) the number from which the Telecommunication originates;
  (ii) the number to which the Telecommunication is sent;
  (iii) if the Telecommunication is diverted from one number to another number, those numbers;
  (iv) the time at which the Telecommunication is sent;
  (v) the duration of the Telecommunication;
  (vi) if the Telecommunication is generated from a mobile telephone, the point at which the Telecommunication first enters a network; but
(c) does not include the content of the Telecommunication.

"Clause" refers to a Clause in these guidelines.

"Customer" means a Person who has a bona fide billing relationship with a Service Provider in respect of a Telecommunications Service.

"European Telecommunications Standards Institute (ETSI)" means the official European standards organisation which produces globally applicable standards for information and communications technologies including fixed, mobile, radio, broadcast and internet.

"Intercept or Interception" has the same definition as defined in the TICA in relation to a private Telecommunication, which means to hear, listen to, record, monitor, acquire, or receive the Telecommunication either:

(a) while it is taking place on a Telecommunications network; or
(b) while it is in transit on a Telecommunications network.

"Interception Access Point" means the Interception point for accessing the call or data.

"Interception Capability" has the same definition as defined in Section 8 of the TICA which

means the capability to Intercept a Telecommunication.

"Interception Warrant" has the same definition as defined in the TICA which means a warrant that is issued to a Surveillance Agency under any of the following enactments:

(a) section 312C or section 312CB or section 312CD or section 312G of the Crimes Act 1961;
(b) section 4A(1) or (2) of the New Zealand Security Intelligence Service Act 1969;
(c) section 15 or section 15B or section 19 of the Misuse of Drugs Amendment Act 1978; or
(d) section 17 of the Government Communications Security Bureau Act 2003.

"Integrated Services Data Network (ISDN)" means a telephone system network.

"ISDN User Part (ISUP)" means a part of the signaling system which is used to set up telephone calls in a Public Switched Telephone Network.

"Law Enforcement Agency (LEA)" has the same definition as defined in the TICA which means the New Zealand Police or any government department declared by the Governor-General, by order in council, to be a Law Enforcement Agency for the purposes of the TICA.

"Law Enforcement Monitoring Facility (LEMF)" means a law enforcement facility designated as the transmission destination for the intercepted communications and call-associated data of a particular Interception subject. The site where monitoring/recording equipment is located.

"Lawful Intercept (or Interception) (LI)" means the Interception of Telecommunications by law.

"Non Coded Access (NCA)" means a service provided by a carrier that results in one of the other carrier's toll access codes being automatically prefixed to a call made by a Customer of the first carrier, where the call is dialled:

- in the format "0 + area code" (the single digit 3, 4, 6, 7 or 9) or "00 + country code"; or
- using one of the non-geographic service codes for mobile Telecommunications Services allocated under the provisions of the number administration deed.

"Network Operator" has the same definition as defined in the TICA which means:

(a) a Person who owns, controls, or operates a public Telecommunications network; or
(b) a Person who supplies (whether by wholesale or retail) another Person with the capability to provide a Telecommunications Service.

"**Party**" means a Person bound by these guidelines under the Telecommunications Act 2001 or a Person signed up to these guidelines.

"**Person**" means a legal Person and includes a company and any other legal entity.

"Public Data Network (PDN)" has the same definition as defined in the TICA which means a data network used, or intended for use, in whole or in part, by the public and includes, without limitation, the following facilities - internet access and email access.

"Public Switched Telephone Network (PSTN)" has the same definition as defined in the TICA which means a dial-up telephone network used, or intended for use, in whole or in part, by the public for the purposes of providing Telecommunication between Telecommunication devices.

"**Service Provider (SP)**" has the same definition as defined in the TICA which means:

(a) any Person who provides a Telecommunications Service to an end-user (whether or not as part of a business undertaking and regardless of the nature of that business undertaking); but
(b) does not include a Network Operator.

"Surveillance Agency" has the same definition as defined in the TICA which means:

(a) a Law Enforcement Agency; or
(b) an intelligence and security agency.

"**Telecommunication**" has the same definition as defined by section 5 of the Telecommunications Act 2001 which means:

(a) the conveyance by electromagnetic means from one device to another of any encrypted or non-encrypted sign, signal, impulse, writing, image, sound, instruction, information, or intelligence of any nature, whether for the information of any Person using the device or not; and
(b) for the purposes of subpart 2 of part 4, includes any conveyance that constitutes broadcasting; but
(c) for all other purposes, does not include any conveyance that constitutes broadcasting.

"**Telecommunications Act**" means the Telecommunications Act 2001 as amended from time to time.

"**Telecommunications Carriers' Forum"** or **"TCF"** means the Telecommunications Carriers' Forum Incorporated Society of New Zealand.

"**Telecommunication(s) Service**" has the same definition as defined in Section 5 of the Telecommunications Act 2001 which means any goods, services, equipment and facilities that enable or facilitate Telecommunication.

"TICA" means Telecommunications (Interception Capability) Act 2004 as amended from time to time.

D. OBJECTIVES AND SCOPE

8. These guidelines will assist all Network Operators and Service Providers to achieve Interception Capability in compliance with the TICA and must be read in conjunction with the TICA; the TICA takes precedence over these guidelines.

9. **Objectives**

The high-level objective is to clarify and expedite the process by which Network Operators and Service Providers comply with the requirements of the TICA.

This objective will be achieved by:

9.1. Ensuring Network Operators and Service Providers interpret the requirements of the TICA in a consistent manner, ensuring the same level of service to Surveillance Agencies; and

9.2. Ensuring individual Surveillance Agencies specify requirements for Interception in a consistent manner.

10. **Scope**

10.1. These guidelines outline a common industry approach to achieving compliance with the TICA ensuring the requirements of any Surveillance Agencies are met in a consistent, cost-efficient and time-efficient manner.

11. **Exclusions from Scope**

These guidelines do **not:**

11.1. Apply to the means of effecting Lawful Interception Capability within the networks of individual Network Operators and Service Providers; or

11.2. Define a compliance implementation strategy. This must be agreed individually by Network Operators or Service Providers with the Surveillance Agencies.

E. TICA GENERAL REQUIREMENTS

12. **Legislative Framework for Lawful Interception**

12.1. The TICA requires Network Operators operating in New Zealand to provide Interception Capability.

12.2. "The purpose of this Act is to ensure:

12.2.1 That Surveillance Agencies are able to effectively carry out the Lawful Interception of Telecommunications under an Interception Warrant or any other Lawful Interception authority; and

12.2.2 That Surveillance Agencies, in obtaining assistance for the Interception of Telecommunications, do not create barriers to the introduction of new or innovative Telecommunications technologies; and

12.2.3 That Network Operators and Service Providers have the freedom to choose system design features and specifications that are appropriate for their own purposes."

12.3. The requirements on Network Operators and Service Providers are defined in part two of the TICA. They include two broad categories:

12.3.1 Duty to have Interception Capability for networks and services; and

12.3.2 Duty to assist.

13. **Network Operator and Service Provider Obligations**

13.1. The requirements of the TICA apply to PSTN and PDN infrastructures.

13.2. Network Operators must ensure public Telecommunications networks and

Telecommunications Services have Interception Capability as follows:

13.2.1 A Network Operator must ensure that every public Telecommunications network that the operator owns, controls, or operates, and every Telecommunications Service that the operator provides in New Zealand, has an Interception Capability.

13.2.2 However, Clause 13.2.1:

a) Does not require a Network Operator to ensure that all components of the public Telecommunications network or Telecommunications Service referred to in that subsection have an Interception Capability; and

b) Is sufficiently complied with if a Network Operator ensures, in whatever manner the Network Operator thinks fit, that at least one component of that network or service has an Interception Capability.

13.2.3 Without limiting Clause 13.2.1 the duty to have an Interception Capability includes the duty to ensure that the Interception Capability is developed, installed, and maintained.

13.3. Notwithstanding Clause 13.2, a Network Operator is not required to have an Interception Capability on a Telecommunication link that is used to interconnect two or more public Telecommunications networks.

F. INTERCEPTION CAPABILITY

14. The objective of this section is to provide guidelines to Network Operators for the implementation of Lawful Interception Capability in their respective network infrastructures.

15. Generic European Telecommunications Standards Institute (ETSI) profiles are to be agreed between the Network Operators/Service Providers and the Surveillance Agencies which will enable the same profile (inclusive of ETSI based options) to be used across all Surveillance Agencies.

16. **International Standards and European Telecommunications Standards Institute (ETSI):**

16.1. These guidelines strongly recommend the adoption of the ETSI international standards that have been specifically developed for Lawful Interception and are commonly adopted in the European and the Asia Pacific region.

16.2. The ETSI standards are regularly updated (approximately annually). It is important to ensure that any new solution being developed conforms to the latest ETSI standards.

16.3. ETSI 102232 is focused on Lawful Interception including:

16.3.1 Handover Interface for Internet Protocol (IP) delivery;
16.3.2 Email services;

16.3.3 Internet Access services;
16.3.4 Layer 2 services;
16.3.5 Multi-media services;
16.3.6 PSTN/ISDN services; and
16.3.7 Mobile services.

16.4. The benefits of adopting these well established standards are:

16.4.1 Manufacturer's technology either currently supports ETSI or is planned for in the near future. This applies to both Network Operators and Service Providers, and Law Enforcement Agencies.

16.4.2 The compliance process will be expedited through all Parties working to common standards and frameworks.

16.4.3 There are efficiencies for the Surveillance Agencies, Network Operators and Service Providers in adopting a consistent approach. This also makes possible the use of common or shared infrastructure where appropriate.

16.5. ETSI standards relevant to Lawful Interception are shown in Annexure 1.

17. Security

17.1. Where feasible all data which is intercepted must be encrypted as follows:

17.1.1 Communications between mediation platforms and Law Enforcement Monitoring Facilities (LEMFs) must use encryption as agreed with the Surveillance Agencies.

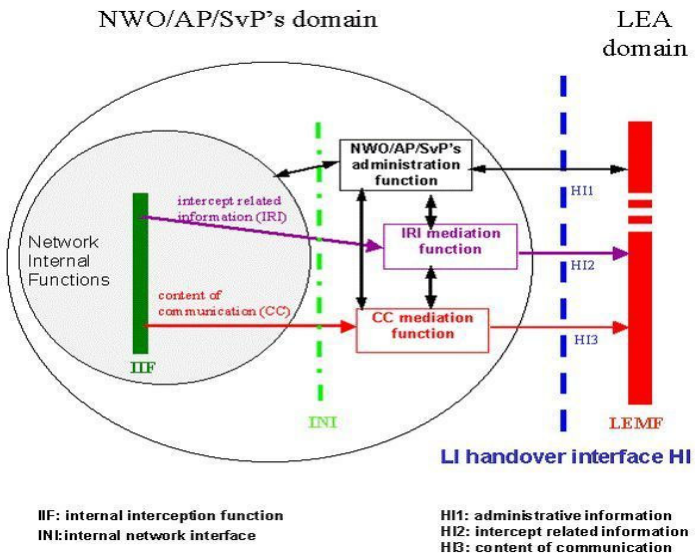
17.1.2 Legal Interception specific or target detailed communications between network elements and mediation platforms must be encrypted using an industry standard algorithm.

17.2. Intra-company communications concerning Lawful Interception matters must be secured and encrypted where possible. All access to Lawful Interception administrative functions must be restricted to the appropriate administrative personnel.

18. ETSI Lawful Interception Architectures

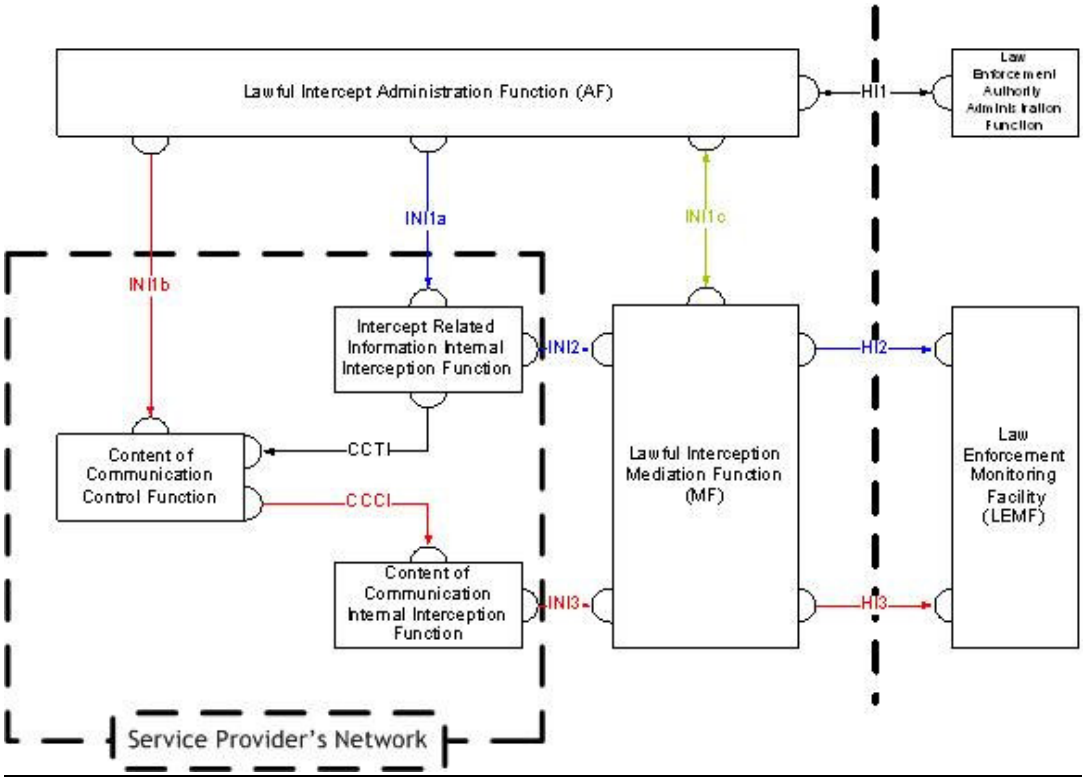
18.1. ETSI TS 101 671 provides a general architectural model for the handover interfaces with the LEMF, see Figure 1.

Figure 1: Functional block diagram showing handover interface HI.



NOTE 1: Figure 1 shows only a reference configuration, with a logical representation of the entities involved in Lawful Interception. It does not mandate separate physical entities.
NOTE 2: The mediation functions may be transparent.

18.2. The following architecture diagram illustrates the implementation of the ETSI Lawful Intercept reference model for an internal Intercept function. There is a description of each component in 18.3, following the diagram.



18.3. The basic elements in this architecture are:

Component	Type	Description
LEAF	Function	**Law Enforcement Authority - Administration Function** This function, manual or automated, transmits a warrant to the Network Operator using the HI1 interface.
HI1	Interface	**Handover Interface 1** HI1 is defined by the relevant ETSI standard for the type of communication being intercepted. The HI1 interface is bi-directional between the Network Operator and the LEA, and provides details for the Interception, usually in the form of a warrant containing specific target information.
LIAF	Function	**Lawful Intercept Administration Function** The administration function receives automated information from the LEA over the HI1 interface, or has manual transmitted warrants entered into it. to set up an interface by the Network Operator. This function is normally provided within the appropriate LI mediation system.
INI1a	Interface	**Internal Network Interface 1a** This is an internal network interface that configures the networks relevant systems to Intercept Related Information (IRI) related to the target. The configuration attributes include information related to internal Intercept identification, target identification information, destination address(es) for intercepted information, etc. These may vary depending on the type of communication being intercepted. The number of systems that may be accessed will vary depending on the type of communication being intercepted.
INI1b	Interface	**Internal Network Interface 1b** This is an internal network interface that configures the networks relevant systems to Intercept content of communication (CC) related to the target. The configuration attributes include information related to internal Intercept identification, target identification information, destination address(es) for intercepted information, etc. These may vary depending on the type of communication being intercepted. The number of systems that may be accessed will vary depending on the type of communication being intercepted.

Component	Type	Description
INI1c	Interface	**Internal Network Interface 1c** This is an internal network interface that configures the LI mediation function to expect IRI and CC information related to the target.
IRI IIF	Function	**Intercept Related Data - Internal Intercept Function** This is the Intercept function within the network used to record and forward IRI data.
CC CF	Function	**Content of Communication - Control Function**
CCTI	Interface	**Content of Communication Trigger Interface** carries trigger information from the IRI-IIF to the CCTF.
CCCI	Interface	**Content of Communication Control Interface** carries controls information from the CCTF to the CC-IIF.
CC IIF	Function	**Content of Communication - Internal Intercept Function** This is the Intercept function within the network used to record and forward CC data, typically on a switch, router or related network element.
INI2	Interface	**Internal Network Interface 2** This internal interface carries IRI data from the network element or system whether IRI data was obtained to the LI mediation platform, including additional details that identify the Intercept target to the mediation platform.
INI3	Interface	**Internal Network Interface 3** This internal interface carries CC data from the network element where Interception occurred to the LI mediation platform, including additional details that identify the Intercept target to the mediation platform.
LIMF	Function	**Lawful Intercept - Mediation Function** The mediation function is sometimes combined with the DF (Distribution Function). Receives both IRI and CC from within the network using INI2 or INI3 interfaces respectively and converts, filters and processes the information to meet the requirements of the warrant before separately providing this information to the LEA through HI2 and HI3 interfaces (respectively).
HI2	Interface	**Handover Interface 2** HI2 is defined by the relevant ETSI standard for the type of communication being intercepted. The HI2 interface is uni-directional from the Network Operator to the LEA, and provides the Intercept related information related to the Intercept.
HI3	Interface	**Handover Interface 3** HI3 is defined by the relevant ETSI standard for the type of communication being intercepted. The HI3 interface is uni-directional from the Network Operator to the LEA, and provides the content of communication related to the Intercept.

LEMF	Function	**Law Enforcement Authority - Monitoring Function** The receiving function within the LEA, it receives IRI and CC from the Network Operator through HI2 and HI3 interfaces (respectively).

18.4. Acquisition Technology

18.4.1 Two general forms of Intercept function are available, internal and external.

a) Internal Intercept functions are software based and sit on routers or gateways in Telecommunication providers networks and can be remotely configured to capture specific information for mediation platforms.

b) External Intercept functions involve the use of probes which are physically separate from but co-located with network elements and interact with mediation devices to pass captured data to LEAs.

With an external Intercept function there are two generic probe deployments, fixed and itinerant.

- Fixed probes are deployed permanently at strategic points in network infrastructure.
- Itinerant probes are those that are not fixed into an operator's network infrastructure. They are installed on an 'as required' basis. Itinerant probes may be owned by the LEA themselves.
- Itinerant probes are connected to a Network Operator/Service Provider's network at an Interception Access Point. These access points can be passive splitters or active network ports. They may be either deployed on demand, or permanently provided where this is required.
- All probes require a transport network to deliver intercepted product to the LEA. For itinerant probes this transport network can either be pre-installed or deployed as required.
- Where Interception Access Points and transport networks are not pre-installed, there can be difficulties meeting the timeliness requirements of the TICA. For this reason it may be appropriate to pre-install this capability at common points where there is a high likelihood of using them.

c) Any Interception technique must be able to support delivery of Interception product to multiple Law Enforcement Agencies simultaneously.

19. Mediation Options

Within the overall architectural model there are two options available for Network Operators to implement the mediation functionality. Either option may be implemented at the Network Operators discretion.

19.1. Network Operator Implemented

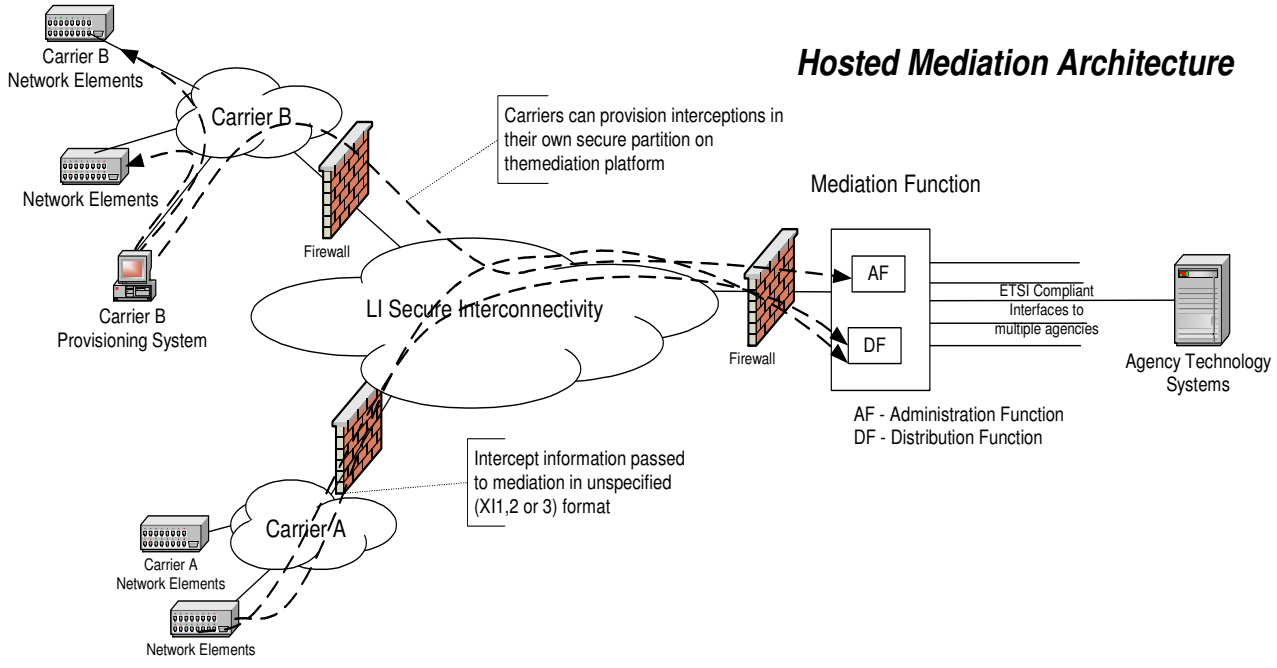
In this case the Network Operator would implement, support and operate the mediation technology themselves. They would reticulate connectivity from themselves to each of the respective Surveillance Agencies.

19.2. Industry Co-operation and Hosted Service

Network Operators have the option to share mediation functionality. However, any such hosted mediation must be approved by all Surveillance Agencies prior to implementation as there may be potential security issues associated with this approach. Architecturally, this would involve individual Network Operators connecting to shared infrastructure.

The shared infrastructure would be hosted by an individual Network Operator or a third party under a service contract. The mediation platform would be securely partitioned to enable Network Operators to have secure individual access.

It is probable that tenant Network Operators would establish connectivity with the respective LEAs via secure logical connections over shared physical media.



20. Call Associated Data

20.1. Call Associated Data can be referred to as IRI (Intercept Related Information) or CAD (Call Associated Data). Various ETSI standards define this in detail.

20.2. Of particular interest in the New Zealand context is the issue of diverted calls. Information about the different parties to these calls is required by the LEAs. This includes at a minimum:

- 20.2.1 The originating telephone number;
- 20.2.2 The telephone number originally called;
- 20.2.3 The telephone number to which the call was ultimately connected; and
- 20.2.4 For mobile phone calls, the cell site to which the mobile phone was connected at the commencement of a call, as a minimum.

Ideally the Surveillance Agencies would like every number involved in a call, but providing that information may not be technically possible.

21. Customer Identifiers

21.1. The TICA anticipates warrants being issued (without limitation) against:

- 21.1.1 A telephone number;
- 21.1.2 A mobile telephone number;
- 21.1.3 A unique identifier for a Telecommunications device (for example an electronic serial number or a media access control address);
- 21.1.4 A user account identifier;
- 21.1.5 An internet protocol address; and/or
- 21.1.6 An email address.

22. Delivering Intercepted Communications to Surveillance Agencies

22.1. The delivery of intercepted communications content to the Surveillance Agency (HI3 in ETSI terminology) should use an ETSI compliant interface. Compliant networks can include:

- 22.1.1 Traditional Telecommunications infrastructure over the PSTN using ISUP trunks. Surveillance Agency delivery trunks must be ISDN to convey the Intercept related information (Lawful Interception Identifier (LIID), etc); and
- 22.1.2 IP networks using streaming content or ftp/sftp delivery.

22.2. ISUP delivery of call content must be able to support sub-addressing or user-user signalling options, preferably both.

22.3. IP delivery of call content and Call Associated Data should be over an encrypted link which meets the requirement of the Surveillance Agency.

22.4. There will be a transitional phase during which delivery of intercepted communication will be maintained using the various mechanisms which are

currently in use.

22.5. If a Surveillance Agency requires the ability to receive intercepted communications for future-emerging applications over an existing interface, the cost of that translation must be met by the relevant Surveillance Agency.

23. **Encrypted Communications**

The obligations for encrypted communications are described in part 2, section 8, paragraphs 3 and 4 of the TICA. The obligations can be described as requiring any communication encrypted by the Network Operator/Service Provider to be decrypted as part of the Interception Capability before delivery to the Surveillance Agency.

24. **Privacy**

The TICA prescribes the privacy requirements in part 1, section 6, and part two, section 8, paragraph 1d.

25. **Duty To Assist**

25.1. Under the provisions of the TICA, Surveillance Agencies may approach Network Operators and Service Providers requesting technical assistance for Lawful Interception. These requirements are contained in section 13 of the TICA.

25.2. There is provision in part 3, section 18 of the TICA for Network Operators and Service Providers to be reimbursed by the Surveillance Agencies for costs incurred in providing this assistance.

26. **Exemptions**

26.1. Section 11 of the TICA provides for exemptions to the other requirements of the Act. Such exemptions can only be granted in special circumstances, for a specified period of time, and may be withdrawn or revoked at any time.

G. PROTOCOLS FOR ENGAGING WITH SURVEILLANCE AGENCIES

27. **General Requirements**

27.1. The TICA is the primary piece of legislation governing Lawful Interception in New Zealand. It is within the portfolio of the Minister of Justice.

27.2. To ensure the integrity and security of Lawful Interception capabilities implemented by Network Operators and Service Providers, any communications with the responsible government ministers is to be conducted in compliance with the protocols outlined in the TICA.

27.3. Any Surveillance Agency as defined in the TICA may request Interception assistance from any Network Operator or Service Provider in New Zealand. Ministerial ownership of the relevant Surveillance Agencies is defined in the TICA.

28. Network Operator/Service Provider Obligations

28.1. Any Network Operator or Service Provider seeking to establish compliance with the TICA shall contact the relevant minister or Surveillance Agency by contacting the administrator via a free call 0800 number 0800LICOMPLY (0800 542 665).

28.2. Network Operators and Service Providers are to submit Lawful Interception compliance plans ("the plans") to the administrator for assessment.

29. Role of the Lawful Interception Administrator

29.1. The Lawful Interception administrator is to:

29.1.1 Act as a point of contact between Network Operators and Service Providers and the Ministry of Justice and Surveillance Agencies.

29.1.2 Facilitate activities as requested by the Surveillance Agencies and the Ministry of Justice. These activities may include:

a) Providing guidance to Network Operators and Service Providers in respect to the preparation of the plans;
b) Managing consideration of the plans by the relevant ministers;
c) Scheduling and managing the conducting of any acceptance testing of proposed capability;
d) Advising on any submissions regarding new technology; and
e) Liaising with the TCF and any of its working parties.

30. Adherence to TICA Requirements

30.1. These guidelines must be read in conjunction with the TICA; the TICA takes precedence over these guidelines.

30.2. The Minister may grant an exemption from compliance with the TICA at his/her discretion as set out in the TICA;

30.3. When a Network Operator or a Service Provider wishes to confirm whether a particular LI solution complies with the TICA The following Process should be used:

30.3.1 Lawful Interception Capability should be demonstrated in accordance with a compliance test plan as agreed with the Lawful Interception administrator;
30.3.2 Compliance testing should be undertaken with a nominated agency (or agencies) as determined by agreement with the Lawful Interception administrator;
30.3.3 Acceptance of the Lawful Interception Capability is to be notified in writing to the Network Operator/Service Provider by the Lawful Interception administrator; and
30.3.4 Any change to the Lawful Interception Capability, as agreed and signed off between Network Operators/Service Providers and Surveillance Agencies, will be at the cost of the Party that

requires the change in order to maintain Lawful Interception Capability.

30.4. It is recommended that Network Operators/Service Providers advise the Lawful Interception Administrator annually or upon the introduction of new technologies which change the network significantly to facilitate ongoing compliance.

H. MONITORING AND ENFORCEMENT OF TICA OBLIGATIONS

31. Monitoring and enforcement of Service Providers or Network Operators TICA obligations is covered under part 3 of the TICA. This section of the Act allows the High Court to make a compliance order if any Person has not complied with any of the duties set out in Part 2 of the Act. The compliance order would require that Person to:

31.1. do any specified thing; or
31.2. cease any specified activity.

A compliance order may be made on the terms and conditions that the High Court thinks fit, including the provision of security or the entry into a bond for performance.

I. EXPIRY, REVOCATION AND AMENDMENT OF THE GUIDELINES

For the avoidance of doubt, and in accordance with the Telecommunications Carriers' Forum's operating procedures manual, any Forum Member may put a project proposal to the TCF's Board (at any time) for the amendment or revocation of the Interception guidelines.

32. Any changes made to the TICA or the ETSI standards may necessitate changes to these guidelines.

Annexure 1

ETSI standards relating to Lawful Interception

Document Number	Title
ETSI ES 201 671 V3.1.1 (2007-05)	Lawful Interception (LI); Handover interface for the Lawful Interception of Telecommunications traffic
ETSI TS 133 106 V7.0.1 (2006-01)	Universal Mobile Telecommunications System (UMTS); Lawful Interception requirements (3GPP TS 33.106 version 7.0.1 release 7)
ETSI TS 133 107 V7.7.0 (2007-10)	Universal Mobile Telecommunications System (UMTS); 3G security; Lawful Interception architecture and functions (3GPP TS 33.107 version 7.7.0 release 7)
ETSI TS 133 108 V7.9.0 (2008-01)	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 7.9.0 release 7)
ETSI TS 101 507 V8.0.1 (2001-06)	Digital cellular Telecommunications system (Phase 2+); Lawful Interception - Stage 1 (GSM 02.33 version 8.0.1 release 1999)
ETSI TS 101 509 V8.1.0 (2000-12)	Digital cellular Telecommunications system (Phase 2+); Lawful Interception - Stage 2 (3GPP TS 03.33 version 8.1.0 release 1999)
ETSI TS 102 232 V1.5.1 (2006-10)	Lawful Interception (LI); Handover specification for IP delivery.
ETSI TS 102 232-1 V2.2.1 (2007-7)	Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; part 1: Handover specification for IP delivery
ETSI TS 102 232-2 V2.3.1 (2007-11)	Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; Part 2: SSD for email services
ETSI TS 102 232-3 V2.1.1 (2006-12)	Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; part 3: SSD for internet access services
ETSI TS 102 232-4 V2.1.1 (2006-12)	Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; part 4: SSD for layer 2 services
ETSI TS 102 232-5 V2.1.2 (2007-12)	Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; part 5: SSD for IP multimedia services
ETSI TS 102 232-6 V2.2.1 (2007-05)	Lawful Interception (LI); Handover interface and Service-Specific Details (SSD) for IP delivery; part 6: SSD for PSTN/ISDN services
ETSI TS 102 233 V1.3.1 (2006-09)	Lawful Interception (LI); Service specific details for email services
ETSI TS 102 234 V1.6.1 (2006-07)	Lawful Interception (LI); Service-specific details for internet access services
ETSI TR 101 944 V1.1.2 (2001-12)	Telecommunications security; Lawful Interception (LI); Issues on IP Interception

Document Number	Title
ETSI TS 102 815 V1.3.1 (2006-04)	Lawful Interception (LI); Service-specific details for layer 2 Lawful Interception
ETSI TS 101 671 V3.3.1 (2008-02)	Lawful Interception (LI); Handover interface for the Lawful Interception of Telecommunications traffic
ETSI TS 101 331 V1.2.1 (2006-06)	Lawful Interception (LI); Requirements of Law Enforcement Agencies
ETSI ES 201 158 V1.2.1 (2002-04)	Telecommunications security; Lawful Interception (LI); Requirements for network functions