



TICSA Interception Standards Consultation: Q and A

1. *What standards do we recommend the Minister references via the Gazette?*

- MBIE recommends that the following standards from the European Telecommunications Standards Institute (ETSI) be referenced via gazette as per Section 42(1).

Title	Description	ETSI standard reference	Comment
Handover interface for the lawful interception of telecommunications traffic	The present document is step 3 of a three-step approach to describe a generic Handover Interface for the provision of lawful interception from a Network Operator, an Access Provider or a Service Provider to the Law Enforcement Agencies.	TS 101 671 v3.13.1 (2015)	This standard is the most recent version.
Handover Interface and Service-Specific Details for IP delivery; Part 1: Handover specification for IP delivery	This standard sets out the handover interface and service-specific details for the interception of IP-services	TS 102 232-1 v3.10.1 (2015)	This standard is the most recent version.
Handover Interface and Service-Specific Details for IP delivery; Part 2: Service-specific details for messaging services	This standard contains service-specific details for the handover of intercepted IP-based messaging services.	TS 102 232-2 v3.8.1 (2014)	This standard is the most recent version.
Handover Interface and Service-Specific Details for IP delivery; Part 3: Service-specific details for internet access services	This standard contains service-specific details for IP delivery, including process of binding a "target identity" to an IP address when providing Internet access, when intercept related information and content of communication needs to be sent, and what information it needs to contain.	TS 102 232-3 v3.3.1 (2013)	This standard is the most recent version.
Handover Interface and Service-Specific Details for IP delivery; Part 4: Service-specific details for Layer 2 services	This standard contains service-specific details for the handover of lawful intercepts for an access provider that has access to layer 2 session information and that is not required to have layer 3 information.	TS 102 232-4 v3.2.2 (2014)	This standard is the most recent version.
Handover Interface and Service-Specific Details for IP delivery; Part 5: Service-specific details for IP Multimedia Services	This standard contains service-specific details for the handover of IP Multimedia Services.	TS 102 232-5 v3.5.1 (2015)	This standard is the most recent version.
Handover Interface and Service-Specific Details (SSD) for IP	This standard contains service-specific details for the handover of the lawfully intercepted	TS 102 232-6 v3.3.1 (2014)	This standard is the most recent version.



delivery; Part 6: Service-specific details for PSTN/ISDN services	PSTN/ISDN Services.		
Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services	This document specifies an approach for the handover of the lawfully-intercepted information that is defined in the two standards: 3GPP TS 33.108 and ANSI/J-STD-025-B. It uses the handover techniques defined in TS 102 232-1.	TS 102 232-7 v3.2.1 (2013)	This standard is the most recent version.
Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI).	This standard specified the handover interfaces for lawful interception of packet-data services, circuit switched services, multimedia services within the UMTS network (GSM-based mobile networks) and Evolved Packet System (the core network of the LTE system).	TS 133 108 v11.4.0 (2012)	This is an older version of this particular standard, which is still widely used.

- Copies of these standards are available at www.etsi.org

2. Will there be exceptions to the referenced standards?

- Sections 10(5) and 24(7) of TICSA define a 'usable format' as either:
 - A. a format that is determined by a notice issued under section 42 (i.e. the gazetted standards); or
 - B. a format that is acceptable to the network operator and the surveillance agency executing the interception warrant or other lawful interception authority.
- To comply with usable format definition 'B' network operators must seek written agreement from the TICSA Registrar that the format and handover used is acceptable.

3. What happens if the referenced standards are amended?

- Section 43 of TICSA states that if a standard is incorporated by reference, there is no automatic obligation for a network operator to comply with any amendments to that standard.
- The effect of this provision is that once a network operator's interception format has been deemed compliant with a gazetted standard, the network operator does not have to change its interception format in response to any amendments to that standard.
- Should a Telecommunication Service or LI Mediation Platform be changed or altered, continuation of existing agreements or validation of compliance is not guaranteed.
- A network operator must ensure that the Telecommunication Service and LI Mediation platform has remained unchanged since they were deemed compliant with a specific gazetted standard, maintaining a written record and declaration to this fact in order to remain compliant with a previous standard.

4. What happens if a network operator was compliant under the previous Act?

- Section 44 of TICSA notes that a network operator that was compliant under section 8(1)(c) of the Telecommunications (Interception Capability) Act 2004, by obtaining the call associated data and the content of telecommunications in a format that was able to be used by a surveillance agency, is not subject to sections 10(5)(c) and 24(7)(a) of TICSA.
- This means that such a network operator may continue to use the interception format that it used immediately before the commencement of section 44 of TICSA. As noted in section 2 of TICSA, section 44 of TICSA came into force six months after royal assent of TICSA on 11 November 2013. The cut-off date under section 44 is therefore 11 April 2014.
- To comply with Section 44 network operators must ensure that the Telecommunication Service and LI Mediation platform has remained unchanged since the commencement TICSA, maintaining a written record and declaration to this fact.
- Should a Telecommunication Service or LI Mediation Platform be changed or altered, continuation of existing agreements or validation of compliance is not guaranteed.

5. How do ETSI standards work (mandatory and optional information)?

- The ETSI standards are broadly comprised of two parts. The first part is a template or schema which is used to convey information; the second part is document which describes the usage of the standard. The two parts must be reviewed together to be of value.
- An example of this for a hypothetical standard:
 - The ASN.1 Schema provides a mandatory field for LIID and an optional field for location. The ASN.1 Schema specifies several ways to define a location, all of which are optional.
 - The ETSI Standard Document stipulates that the LIID (LawfulInterceptionIdentifier) must always be populated, and that for some given network events a Location field must be provided. As there are several ways to define a location within the ASN.1 Schema, at least one of the location fields/definitions must be populated for the given network events.

6. What is covered by the national variant?

- ETSI standards allow national variants to enable jurisdictions to place additional requirements above those stipulated by ETSI. National variants are also used to remove ambiguity and to clarify details about optional variations and fields within the standards. It is the latter which is proposed herein.

Location:

- For those events / scenarios where the standard used stipulates that a location must be provided (or is provided by the network operator where it may be optional), the following clarifies the location information which is acceptable to determine the point a call enters the network.
- The location must determine the target's physical location where the network operator is providing the 'last mile'/access:
 - Geographic coordinates* of the target; or

- **Physical street address (or Geographic Coordinates*) of the 'fixed access' the target has used to established the current connection; or
 - **Geographic coordinates*, azimuth (direction) and practical range of the Network Operator's antenna for which a target is connected to wirelessly).
- Those instances of a service where the network operator does not provide 'last mile'/access, the location information must provide registration details which identify the target to the Network Operator for the associated service e.g. SIP Registration, IPAddress.

*Geographic coordinates as defined MapDatum - WGS84.

**A network provider is able to satisfy this requirement by supplying (in advance) the LEA with data which can be used to derive the physical location information of the target and/or network equipment from the attributes supplied in the IRI E.g. Suppling a document in advance which correlates a globalCellId attribute (as supplied in IRI) to a physical BTS/Cell Site, antenna direction and its associated coverage pattern.