WHITE PAPER

CSP Regulatory Solutions

Network visibility solutions for operator legal compliance

KEYSIGHT

Introduction

The UN ITU Declaration of Principles on Building the Information Society reaffirms Article 29 of the Universal Declaration of Human Rights in that everyone shall be subject to limitations determined by law solely for the purpose of securing respect for the freedoms of others and for meeting the just requirements of public order and general welfare in a democratic society.

The Budapest Convention on Cybercrime is a global treaty drawn up to harmonize international law to meet the objectives of Article 29 in an information society. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, by adopting appropriate legislation and fostering international co-operation. The treaty has been ratified by 68 countries.

The treaty outlines three circumstances where a service provider provides assistance to government by disclosing data.

Service providers are legally obliged to comply with lawful intercept warrants, data disclosure requests and production orders to provide government assistance. In addition, they have obligations to notify agencies of cybersecurity incidents and have forensic readiness to support investigations into threats to critical infrastructure on public networks. To support operators' regulatory requirements, Keysight's visibility products can select traffic for interception feeds and generate the metadata required to support cybercrime investigations.

Compliance with Lawful Demands

The legislative framework in the treaty defines four types of legal orders that may be served on a service provider.

Measure	Obligation on service provider
Preservation Order	Compels a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that party traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
Disclosure Request	Compels a service provider in the requested party's territory to produce specified and stored traffic data in that service provider's possession or control which is needed for the party's specific criminal investigations or proceedings
Production Order	Compels a service provider to disclose specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing party's specific criminal investigations or proceedings
Interception Warrant	Compels a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that party content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

Voluntary Engagement

Service provider networks and the subscribers and critical infrastructure that depend on them are under threat from nation state actors and organized crime groups. To defend the networks and subscribers, operators will share threat intelligence with government agencies and request their specialist assistance to ensure resilience or investigate high-end threats through forensic analysis. To ensure that privacy and data protection obligations are upheld the same level of data disclosure thresholds are applied.

Although the sharing of threat intelligence is voluntary there is legislation and industry standards that compel service providers to generate and retain logs of activity in their network.

Legislation or standard	Relevant section
NIS2	The operator sets up a logging system on each information system to record events relating, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the information system.
ISO27001	9.1 Monitoring, measurement, analysis and evaluation A.12.4 Logging and monitoring A.14.1.2 Securing application services on public networks A.15.2.1 Monitoring and review of supplier services A.18.1.3 Protection of records
NIST Cyber Security Framework	ID.RA-1, ID.SC-1, PR.MA-1,2, DE.CM-1,2,3,6,7 DE.AE–3, RS.MI-3, PR.PT-1
European Electronic Communications Code Article 40	SO.21 SO.23
GSMA Fraud and Security Group	FS.31 Security manual RI-004 NO-007 FS.11 SS7 FS.19 DIAMETER FS.20 GTP-C FS.22 VoLTE FS.37 GTP-U
UK Telecoms Security Act 2021 Code of Practice	18.06 18.07 18.09 18.12 18.17
US Executive Order 14028	8 EL1

These logs provide essential information to incident response teams to identify and scope incidents and develop effective countermeasures.

Emergency Assistance

Service providers operate public networks, and the treaty makes provision for government to request assistance in circumstances where there is a threat to life or a major risk to public safety. Subject to the appropriate authorization, service providers can disclose communications data or subscriber information or location when emergency assistance is requested. Example scenarios for location data requests are locating kidnapping victims or missing persons. Communications or subscriber data could be requested to identify compromised nodes during a distributed denial of service attack.

Conversely, there is the situation where subscriber directly requests assistance from government services using the service provider's network. The most obvious example is the 911 emergency service number. The 911 service has evolved over 55 years from a dedicated connection to the operator to the complex routing and dispatch system implemented today with the following features:

Requirement	Feature
Positioning	Network assisted geolocation of emergency caller
	In-band delivery of emergency caller location to dispatcher
Call Routing	Location based routing of call to dispatcher
	Callback from dispatcher
	Routing for inbound roamers
Resilience	Fallback to circuit switched from VoIP
	eCall. Automatic call after accident with delivery of vehicle data
	Operation without SIM

The 911 service has stringent regulatory oversight for resilience and performance with financial penalties for non-compliance or outages.

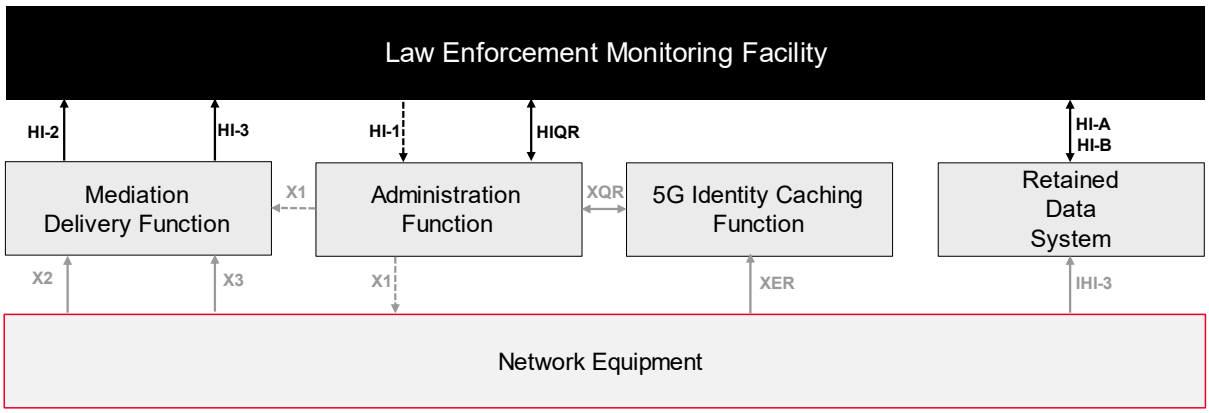
The final use case for emergency assistance is providing access to first responders. Modern mobile networks are far more sophisticated than previous critical communication networks with much lower terminal costs. 3GPP has delivered standards for the implementation of critical communications such as push-to-talk service and side-linking between devices. Large amount of government funding has therefore been given to service providers to fill coverage gaps and provide priority access for first responders. Examples are US FirstNet (First Responder Network Authority) and the UK Emergency Services Network (ESN). The multi-billion dollar sums involved in these contracts demands service level agreements (SLAs) driven by network key performance indicators (KPIs).

Lawful Disclosure Systems Ecosystem

To assist operators to meet legal obligations the industry response had been a set of standards to ensure interoperability of the data lawfully disclosed by operators to government. They define how to implement the technical support in networks to support the assistance requests. These standards are commonly referred to as Lawful Intercept / Retained Data (LI/RD) specifications. ETSI has leadership for the handover interfaces in the TC-LI group and 3GPP standardizes the implementation of LI/RD in mobile networks in the SA#3 group.

Keysight is unique in the visibility industry in being a member of the 3GPP and ETSI standards groups. This drives engagement with the LI/RD mediation vendors, government stakeholders and service providers in the TC-LI committee. Strict adherence to the LI/RD standards minimizes integration issues with mediation partners and provides safe harbour for the service provider that the solution is traceable to global standards.

The 5G LI architecture and functions are defined in ETSI TS 133 127 with the protocols connecting the functions defined in ETSI TS 133 128. The RD architecture and functions are defined in ETSI TR 103 657 with the protocols connecting the functions defined in ETSI TS 102 657.



The top layer of the stack is the **LEMF** – Law Enforcement Monitoring Facility. This is hosted at a government agency which issues intercept warrants, preservation orders, production orders and disclosure requests. The LEMF processes the intercept product and disclosed data. Communication with operators is via handover interfaces standardized by ETSI.

- **HI-1** – Tasking Interface – Prior to 4G intercept warrants were paper or fax requests to operators containing the subscriber identifiers to be intercepted. To automate this process the ETSI TS 103 120 eWarrant interface is now specified.
- **HI-2** – Intercept Related Information (IRI) – IRI is interception metadata such as parties in the call and network identifiers. This handover uses the ETSI TS 102 232 interface based on ASN.1 encapsulations.
- **HI-3** – Communications Content (CC) – The intercepted content is also encapsulated in ETSI 102 232 to deliver voice or data to the LEMF.
- **HIQR** – Handover Interface Query Response – In 5G only temporary or concealed identifiers are exchanged over the air. To support production orders that cite these identifiers and require the permanent identifier an identify association capability was added to the LI architecture in 3GPP 33.127. The query and response formats are defined in 3GPP 33.128 and use the ETSI TS 103 120 eWarrant interface to the LEMF.
- **HI-A / HI-B** – Disclosure requests for communications data are passed over the 'A' interface and disclosed communication data records are handed over to the LEMF on the 'B' interface. These interfaces are defined in ETSI TS 102 657 which specifies ASN.1 and XML encoding and TCP and HTTP transports.

The infrastructure at the service provider that communicate with the LEMF via the handover interfaces are termed mediation functions. These functions are managed by the operator and subject to strict security controls and regulatory oversight.

- **ADMF** – Administration Function – The ADMF processes the HI-1 interception warrants and HIQR identity requests. Identity requests are forwarded to the identity caching function via the internal XQR interface using the ETSI 103 221 protocol. Intercept warrants are processed by a LI provisioning function (LIPF) and task the sources of IRI and CC via the internal X1 interface.
- **ICF** – Identity Caching Function – The ICF receives a stream of identity records on the XER interface that give the binding between temporary identifiers such as the GUTI or Cell ID, permanent identifiers such as SUPI/IMSI or IMEI and concealed identifiers such as the SUCI. The ICR stores these records and handles queries on the XQR interface.
- **RDS** – Retained Data System – The RDS processes disclosure requests on the HI-A/B handover interface to retrieve the stored the communications data using the selection criteria in the request. The communications data is pushed from data collection functions via the IHI-3 interface to be stored and indexed on the RDS. The service provider "owns" the data in the RDS and is responsible for the data protection obligations under the relevant legislation.
- **MDF** – Mediation and Delivery Function – The MDF delivers intercepted metadata and content received on the X2 and X3 interfaces to the HI-2 and HI-3 handover interfaces. The MDF translates the standard 5G interfaces to the required national variant of the handover interface.

The internal interfaces between the mediation functions and the sources of CC, IRI, identity association events and communications data have undergone partial standardization in the 3GPP 33.127 and 33.128 specification to encourage vendor diversity using the ETSI TS 103 221 interfaces.

- **X1** – Interception is provisioned using the ETSI TS 103 221-1 protocol with XML data and HTTP transport. This interface also supports hashed identifiers to avoid having target lists stored on points of interception.
- **X2** / **X3** – Intercepted metadata and content are streamed to the MDF using the ETSI 103 221-2 encapsulation. This is binary tunnelling protocol that encapsulates the intercepted packets with interception metadata such as timestamps.
- **IHI-3** –ETSI TR 103 657 defines a reference interface between data collection function and data storage functions. No protocol is defined but the intent is to define a reference point where communications data is reduced to the minimum number of fields to meet data disclosure obligations.
- **XER** – 3GPP 33.128 defines an ASN.1 BER message stream that contains association and disassociation updates between permanent identifiers and temporary identifiers.

In most cases these internal interfaces are implemented by the network elements to provide turn-key integration with the mediation functions. There are, however, some gaps due to emerging government requirements or traffic routing where there is no point of interception on the equipment. In these cases, network visibility data can be used to feed the newly defined LI/RD elements listed below.

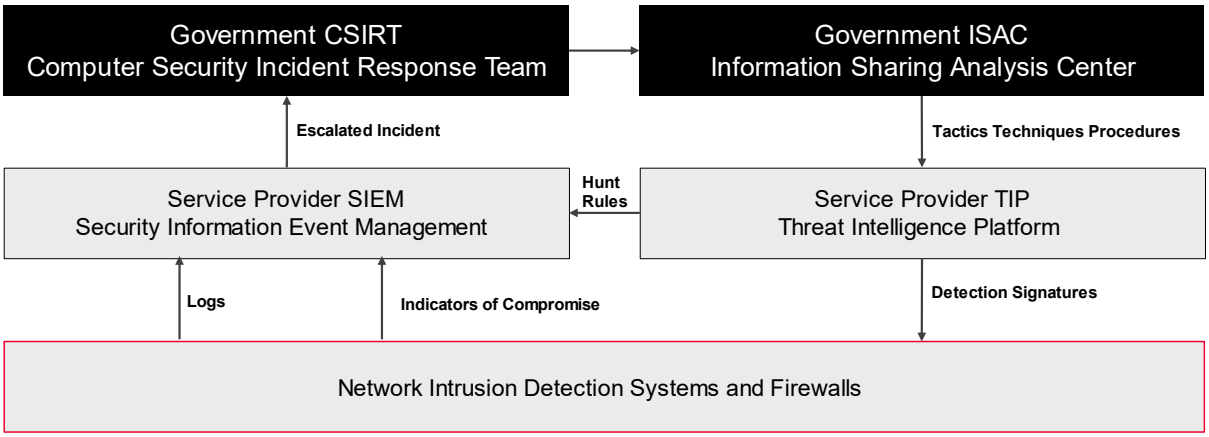
- **LMISF** – LI Mirroring IMS State Function –To minimise interoperability issues home routing via S8HR or N9HR is the preferred implementation of roaming voice. For LI/RD this means that the intercept points in the IMS core are bypassed by inbound roamers. 3GPP 33.127 specifies an LMISF function that receives VoLTE/NR signalling and media streams on X2-LITE and X3-LITE interfaces from a BBIFF (Bearer Binding Intercept Forwarding Function). The LMISF uses targeting information on X1 and delivers metadata and content on X2 and X3. The BBIFF routes GTP bearers carrying SIP and RTP media to X2-LITE and X3-LITE. The LMISF is implemented as a virtual function and the BBIFF can as a network visibility function.
- **IPAR** – IP Address Resolution – Service providers must support both IPv4 and IPv6 UEs and need to be able to connect them to both IPv4 and IPv6 internet servers. The exhaustion of IPv4 addresses necessitates the use of network address and port translation at the internet peering point with both NAT44 and NAT64 required. This arrangement is commonly referred to as CGNAT (carrier grade NAT). If a production order cites a public network address/port, for example, in a set of access logs seized from a server containing illegal content then the service provider is responsible for resolving the private IP address that was translated and giving the subscriber identifier associated with it. A network visibility function can select the essential packets required to correlate the private and public IP addresses and ports.
- **DCF** – Data Collection Function – An emerging requirement in many jurisdictions is the capability to generate communication data records (CDRs) for user plane activity and bind this to permanent identities. Often termed internet communications records (ICRs) this metadata contains DNS activity, certificate information and source and destination address of web transactions but never content. The DCF is defined in the ETSI TR 103 657 architecture. Its role is to collect CDRs in IPFIX format from network visibility functions.

Keysight's role in the lawful disclosure ecosystem is to provision filtered traffic and metadata feeds on its network visibility solutions to provide the data required by the newly defined LI/RD elements which have no support in network elements.

Voluntary Disclosure Systems Ecosystem

Cybercrime is extremely attractive to organized crime gangs because of the low probability of arrest and the high financial returns. This also drives collaboration with nation states who have the same objectives for political ends. The consequence of this environment is that service provider subscribers and the carrier networks themselves are under constant threat from high-end cyber actors. The subscribers most under threat are typically high-end enterprise clients that have subscribed to managed security services to defend their infrastructure and personal data. The potential reputational damage and associated consequential losses of an incident are a strong incentive to share intelligence on malicious activity with government and to act promptly on government threat intelligence.

Unlike the LI/RD ecosystem there is no formalized architecture for the sharing of threat intelligence, however the diagram below gives context to the roles of government and service providers and the information flow between them.



The top layer of the stack is the operations division of the national cyber agency such as DHS CISA in the USA or the NCSC in the UK. There are two key roles of this agency.

- **CSIRT** – Computer Security Incident Response Team – This group receives incidents and forensic data from service providers and analyses it to judge its impact and the appropriate response.
- **ISAC** – Information Sharing and Analysis Center – The incident response guidance from the CSIRT is aggregated and classified for dissemination with industry security teams. There are also national ISACs for industry verticals such as health, energy, and transportation that a service provider might receive threat intelligence from to defend its subscribers in these verticals. Lastly, there is also a dedicated T-ISAC for telcos that provides a threat intelligence service for carrier interconnects managed by the GSMA.

The functions at the service provider that interact with the national cyber agency are defined in the NIST Cyber Security Framework (CSF) with the relevant categories being analysis and communications.

- **RS.AN** – Analysis - Analysis is conducted to ensure effective response and support recovery activities.
- **RS.CO** – Communications - Response activities are coordinated with internal and external stakeholders (e.g. External support from law enforcement agencies).

The supporting systems for these functions are SIEM and TIP for analysis and communications categories respectively.

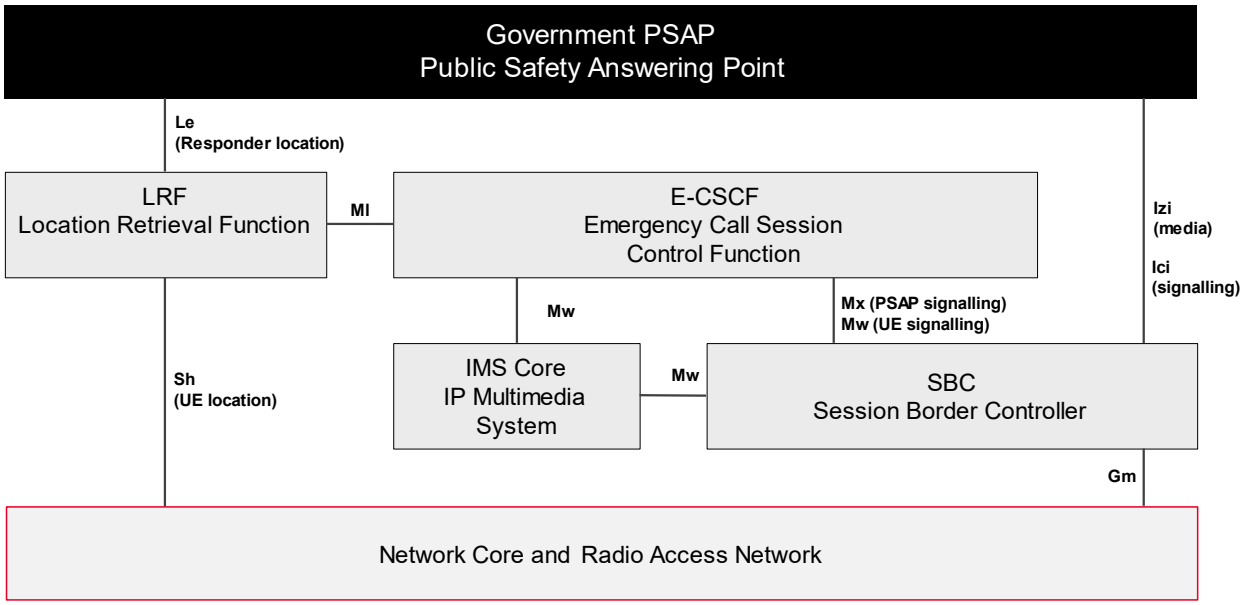
- **SIEM** – Security Information Event Management - SIEM systems collect alerts from host or network-based intrusion detection systems or analyse log data for potential threats. Typically, the system will provide and automated workflow to allow the security operations analyst to focus on the critical threats. Incidents deemed a potential threat to national security are escalated to the CSIRT.
- **TIP** – Threat Information Platform – These systems exchange threat intelligence with ISACs and provide a platform to visualize, analyze and correlate threats. MISP (Malware Information Sharing Platform) is a commonly used opensource platform that also has its own data model and federation protocol. Notable MISP users in the communications industry are the ISACs for NATO, GSMA and PISAX (IXPs and GRXs). TIP systems can also distribute threat hunting and detection rules with notable formats being Yara for binaries, Snort for network intrusion detection and Sigma for system logs.

The volume of threats demands secure electronic exchange of threat intelligence. The intelligence must also be structured to enable automated analysis. TAXII (Trusted Automated eXchange of Indicator Information) has emerged as a standard for secure exchange of threat intelligence. It's counterpart for a structured data model of threat intelligence is STIX (Structured Threat Information eXpression). Both standards were developed by DHS CISA and have been adopted by other governments such as the UK. Policies on what information can be shared and with who are required so a framework has been developed by FIRST (Forum of Incident Response and Security Teams). The most notable is the Traffic Light Protocol (TLP) to annotate threat intelligence with sharing boundaries to be applied by recipients.

Keysight's role in the voluntary disclosure and threat intelligence ecosystem is to provision filtered traffic to network intrusion systems and to feed logs of network metadata to SIEM systems for analysis.

Emergency Assistance Ecosystem

The point of contact with government from the service provider is the PSAP (Public Safety Answering Point)

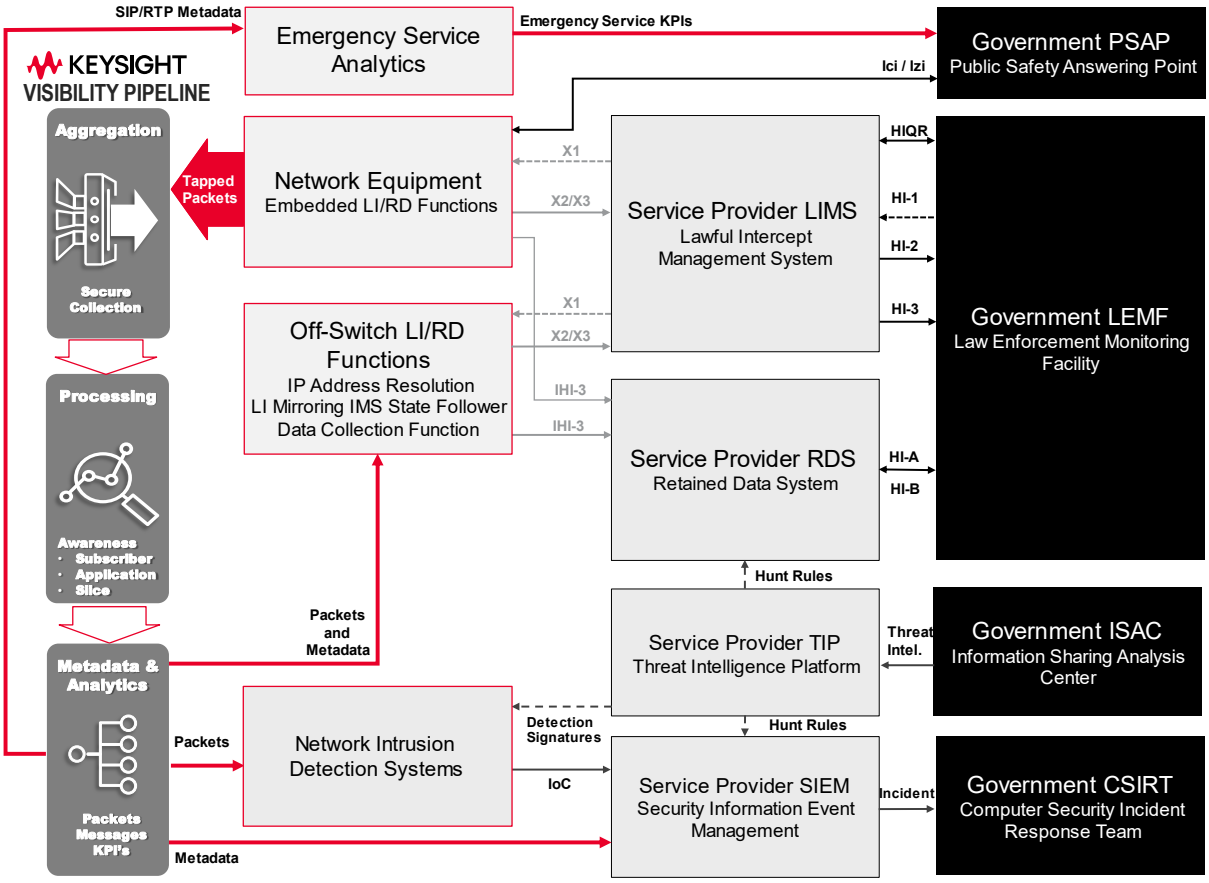


Keysight's role in the emergency disclosure and public safety ecosystem

Keysight Data Pipeline for Govt. Assistance

The Keysight visibility data pipeline provides comprehensive visibility of the user and control planes in fixed and mobile networks using both physical and virtual network taps. These packet streams are secured and forwarded to packet brokers with custom silicon for terabit processing throughput. Visibility of the control plane ensures that Keysight packet brokers are subscriber aware and can both filter traffic based on a subscriber identity and produce user plane metadata records that are enriched with identities.

The Keysight visibility data pipeline can implement LI point of interceptions (POI) and RD data generation functions. This is enabled by subscriber awareness which ensures that the filtered packets and metadata is limited to the subscribers cited in the assistance request. This concept also applies to telco network defense operations in which the visibility data pipeline feeds intrusion detection systems and the metadata can be logged to SIEM systems. Finally, the pipeline can select emergency call data for analytics system that derive KPIs.



This approach enables service providers to reuse their existing network taps and the capabilities of Keysight's visibility data pipeline to address government assistance obligations.

Keysight is the only visibility provider whose equipment is used for performance, security, and interoperability tests. Our focus on metrology grade hardware and software performance is applied to ensure that our visibility solutions can meet the stringent requirements for handling evidential data.