BAE SYSTEMS

BAE Systems DataBridge™

Helping Communications Service Providers comply with Lawful Interception regulations

Complying with Lawful Interception regulations

As terrorists and organised criminals make increasing use of social media and smartphones to facilitate their crimes and activities, the data they generate and which is transported by Communications Service Providers (CSPs) is of growing value to public authorities charged with monitoring threats to society, detecting crimes and investigating and prosecuting criminals.

In response, national legislation now commonly supports the rights of authorities to access the metadata (signalling information) and content associated with communications between individuals (Subjects of Interests [SoIs]) who may be targeted in the pursuit of authorised investigations.

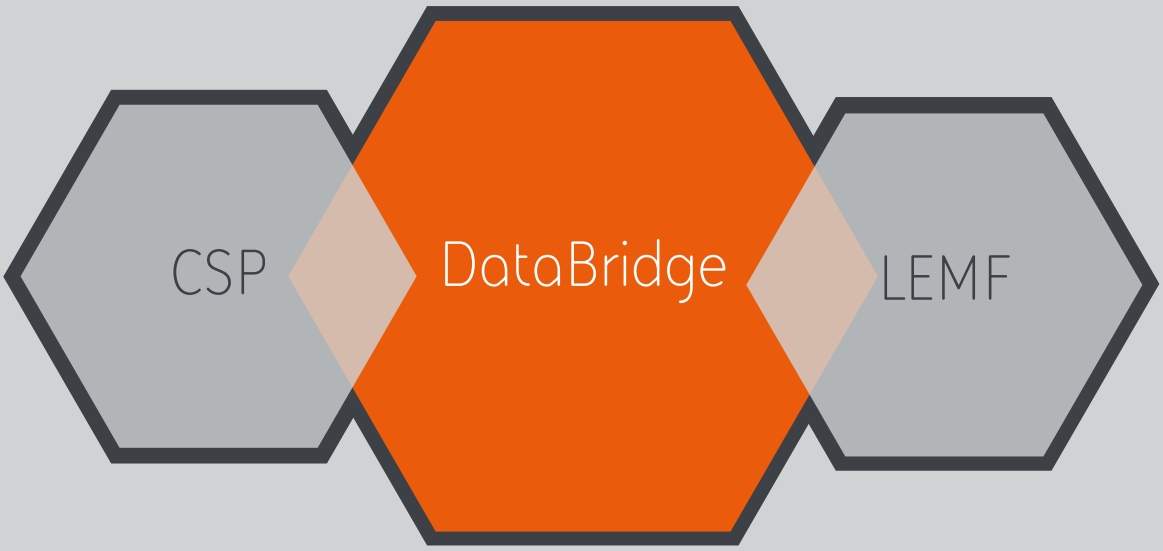
For CSPs, this means that they must be prepared to comply with authorised requests from Law Enforcement Agencies (LEAs), to lawfully intercept the communications associated with targeted SoIs, and for a pre-specified duration, provide metadata (signalling information) and content for all their communications to LEAs, either in real-time or delivered afterwards as part of a packaged file transfer.

However, depending upon the type of communication (e.g. Voice/Data/VoIP/Video) or the device utilised (e.g. telephone/smartphone/tablet), communications from individual SoIs can be distributed across different telecommunications infrastructures, transiting different switches (physical and software) and gateways. This all adds complexity for the CSP, who, regardless of how the SoI choses to communicate, must comply with legislation to intercept the communications from their networks using Active or Passive means and relay content data and metadata/signalling information to the Law Enforcement Monitoring Facility (LEMF) of the requesting LEA. This process is often further complicated when different LEAs, possibly under different regulatory frameworks, request information relating to the same SoI: the CSP must deliver the correct data, and only the correct data, to the correct LEA, securely, with provision of an audit trail detailing all activity. And at all times, the CSP must respect the privacy and security of their subscribers and their data. All in all, it's quite a challenge.

The Solution

DataBridge from BAE Systems

BAE Systems DataBridge is a purpose built, proven Lawful Interception (LI) solution for CSPs who must comply with local LI legislation, serving information requests from multiple LEAs from a common platform. It is easy to deploy, simple to use, and fully automated, helping CSPs to cost effectively achieve LI compliance.



The solution bridges the gap between the CSP and the LEA, and provides the following capability to help relieve the burden of compliance by automating resource consuming administrative tasks and repetitive LI operations:

Acquisition of data: It is the responsibility of the CSP to gather ('acquire') the targeted SoI data from its network so that this data can then be forwarded in real-time to the LEA, as authorised by a legal warrant from the LEA. Data is gathered from the network at Intercept Accept Points (IAPs), which can be a CSP Network function with an LI capability, a dedicated LI probe, a switch port mirror or a third party Lawful Interception Gateway (LIG).

The BAE Systems DataBridge solution supports both Active and Passive modes of data gathering from the IAPs in a CSP's network:

- **Active acquisition:** Metadata and Content is copied by the Network Functions, gateways or other devices in the network and forwarded in real-time to the components of the DataBridge solution that deal with SoI traffic selection, Identifier correlation, Mediation and Handover to the LEA. Within many Network Functions, active interception is supported as part of the core capability. BAE Systems DataBridge can interface with these infrastructure components and manage the targeting of required data.

- **Passive acquisition:** Where needed, capability (hardware or software probes) can be provided to passively intercept the communications of targeted SoIs within networks, to copy the content, related signalling information and metadata of those communications, and forward them to a central processing (mediation) solution. Although traditionally more expensive, this capability is often preferred where the capability for LI is to be performed with minimal disruption to the CSP, or where the LEA takes ownership of the LI process.

Mediation and Handover Solution: A collation and processing solution that gathers and collates data forwarded in real-time from the various Intercept Access Points (IAP) into a centralised or distributed facility, maps data to LEA warrants, converts the data to the standard output format mandated by regulations and as required by individual LEAs[1], and in real-time forwards targeted communications content and metadata/signalling information to the correct LEMF in accordance with the requested standards-based handover specification[2].

Where necessary, the solution also performs automatic redaction of non-authorised content or metadata elements before transmission to LEAs, and if in receipt of encryption keys from the CSP, can remove any CSP specific encryption, thus providing the data to the LEMF in a readable format.

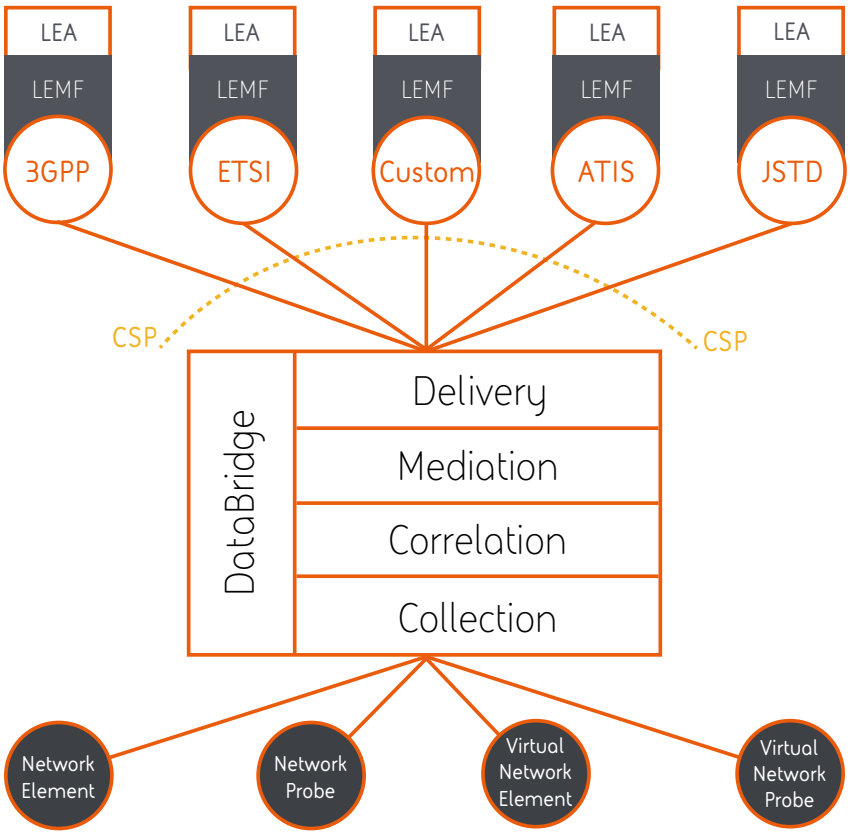
Where required, the IAP and LEMF interfaces can be encrypted in either TLS or IPSEC, ensuring private and secure end-to-end communication between the IAP and the LEMF.

Management: A capability to provide centralised management of IAPs and other third-party Mediation Solutions, providing remote management and tasking of IAPs (e.g. switches/probes/routers) to actively collect targeted communications, with additional management of other legacy mediation solutions, such that their output becomes input to the overarching DataBridge solution.

Where required, and to ensure continuous LI compliance at all times, the BAE Systems DataBridge solution can be deployed in a highly available architecture, providing a fault-tolerant redundant system.

- **Warrant management:** DataBridge offers both an intuitive Web GUI for Warrant and Intercept management and a Warrant Management API allowing DataBridge to be integrated into other warrant management systems.

- **Provisioning:** DataBridge provisioning can manage the tasking of IAPs with the necessary target information: this can either be as provided through the Warrant Management interfaces or as derived from the DataBridge Correlator. The Correlator takes inputs such as Radius or DHCP and matches the provided SoI information with real-time session information to determine the appropriate target identifier which is then applied to the IAP. DataBridge provisioning can also be configured to continually audit IAPs to ensure the current and desired tasking states are aligned.



Extensive IAP Support

With a global presence and 25 years of LI experience, the BAE Systems DataBridge solution has built up a comprehensive library of IAP interface modules covering a wide range of access technologies, equipment vendors, switch types and software versions, with new modules being added all the time.

DataBridge is a proven solution for both fixed and mobile technologies.

For mobile voice and data services, DataBridge provides capability for all access and core technologies including GSM, UMTS, LTE and IMS plus support for the latest NFV and SDN architectures.

For fixed line and broadband services DataBridge covers xDSL, cable, fiber, wireless, satellite and voice services (IP and TDM).

Comprehensive standards conversion capability

Similarly, BAE Systems DataBridge's global footprint means mediation modules are maintained for all internationally recognised LI standards bodies, as well bespoke capabilities for many country specific implementations.

High Speed Mediation

DataBridge can be deployed to meet the most demanding throughput requirements, performing traffic selection on 100Gbps links, while offering single target mediation of up to 10Gbps. These capabilities combined with the limitless scaling architecture provided by the virtualised BAE Systems DataBridge vLI solution, ensures the BAE Systems DataBridge offering meets the throughput requirements of today and tomorrow.

Technical Specifications

Network Equipment Vendor Support

Huawei, Cisco, Oracle, Mitel, Nokia, Ericsson, ZTE, BroadWorks, Samsung, Juniper, Genband, CASA, Comverse, Sonos

Networks & Services

- PSTN
- GPRS, GSM, UMTS, CDMA, CDMA2000, LTE, VoLTE
- XDSL, Cable
- WLAN
- SMS, MMS, Voicemail
- PoC (Push-to-talk over Cellular)
- VoIP (SIP, RTP, H.323, SCCP)
- Internet Access (IPv4 and IPv6)
- Email (POP3, SMTP, IMAP, webmail)
- Additional IP-based services

Network Interfaces

10/100/1000 Mb Ethernet, 10/40/100 Gb Ethernet, ISDN, ATM, E1/T1, SS7 Interfaces

Performance

- A scalable solution, with no limit on the number of targets, LEA or network element connections
- 10Gbps per target mediation and delivery throughput with no limitations on total mediated throughput for the DataBridge vLI software option

Support for LI standard created by the following telecommunication standards bodies:

- ETSI, 3GPP, ATIS, J-Standard, Packet Cable, TIA

BAE Systems DataBridge also supports county specific overlays to any of the above standards.

Making DataBridge work for you

The ability to support the real-time lawful interception of communications is now a core requirement of all CSPs who operate under government licences, with LI considerations extending across all their communications services. As the sheer volume of communications grows, so too will the burden this places upon CSPs, requiring them to ensure that their LI solution has the capability and capacity to scale in line with subscriber growth. Furthermore, as technology evolves, the speeds with which LI solutions must capture, process and mediate data and then transmit it in real-time to LEMFs will continue to increase. It is also anticipated that as new communications services are developed and deployed, LI regulations will adapt and be extended to encompass changing technology and communications methods. Clearly, CSPs must always adequately plan for the future, ensuring that any new consumer or enterprise services to be launched will also be compliant to LI requirements, lest competitive advantage be lost, while the situation is rectified.

With respect to the above, not only does the BAE Systems DataBridge solution address the challenges of today, but it also addresses the demands of tomorrow: the BAE Systems DataBridge solution is a scalable, reliable and flexible future-proof solution for CSP Lawful Interception compliance with capability to provide high-speed mediation throughput of targets up to 10Gbps.

And as CSP architectures change and more communications infrastructure is virtualised and moved to the cloud, the DataBridge solution can continue to provide reliable LI support, through implementation of our new virtualised BAE Systems DataBridge vLI capability.

BAE Systems has been specialising in Lawful Interception for 25 years. We are a trusted partner of CSPs and LEAs around the world, with solutions in place in over 15 countries.

To learn more about BAE Systems DataBridge, High-Speed Mediation, our NFV and SDN compatible virtualised LI (vLI) solution, our training capability for CSP LI operators, our Telco Compliance consultancy services, our customised LI offerings, or our CSP Service Level Agreements, please contact us.

We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

BAE Systems
1 Raffles Place #23-03, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST
CESG Certified Service
Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure