

BAE Systems DataBridge

A proven lawful intercept solution for communications service providers and law enforcement



Digital
Intelligence

BAE SYSTEMS

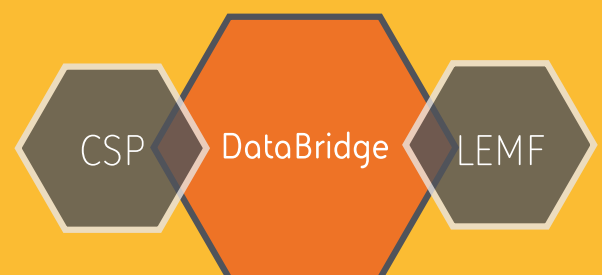


BAE Systems and DataBridge Lawful Interception

As terrorists and organised criminals (Subjects of Interest (Sols)) make increasing use of the internet, social media and smartphones to facilitate their crimes and activities, communications service providers (CSPs) are under scrutiny like never before. The data Sols generate whilst communicating or conducting their activities is transported by CSPs across their networks, and is of significant value to law enforcement and national security agencies, for whom it forms a key element in their efforts to monitor threats, detect crimes, investigate and prosecute criminals and save lives.

To assist agencies in gathering information on the activities, contacts, locations, behaviours and intentions of Sols, CSPs must comply with the lawful intercept (LI) mandates of their host nations. In response to a lawfully authorised request, a CSP is required to intercept and copy the real-time communications of targeted Sols, such as voice, data and messaging and forward this data in the required format to the LEA controlled Law Enforcement Monitoring Facility (LEMF). At all times, CSPs must ensure protection of the data, ensuring that no unauthorised user has access to it, and that only the correct, authorised data is ever provided in response to each individual LEA warrant.

LI is an essential tool in the LEAs fight against crime and terrorism. As CSP networks expand and adopt newer more complex technologies, maintaining compliance to national requirements becomes increasingly challenging. For CSPs, the cost of LI must be borne as a cost of doing business. To prevent it becoming a cumbersome burden that side-lines resources and hinders normal business processes, it is prudent to partner with an LI expert who has a proven industry track record in LI and can help them fulfil their compliance requirements.



Helping CSPs comply seamlessly and efficiently

BAE Systems has almost 40 years of experience working with CSPs to help them meet their regulatory obligations for LI in a timely and efficient manner. Our solution, BAE Systems DataBridge, is a proven industry standard solution for lawful intercept. It delivers high performance LI capability to fixed, mobile and satellite communication networks.

Upon receipt of an authorised warrant, DataBridge system operators use an intuitive web-based management interface to simplify and facilitate the configuration of CSP infrastructure to collect the required real-time content and metadata of targeted Sols. The solution will manage the receipt of that data from the CSP's network infrastructure, the formatting of the data according to LEA requirements, and the forwarding of the data to the appropriate LEMF. The solution facilitates effective management of LEA warrants and ensures an audit trail of activity.

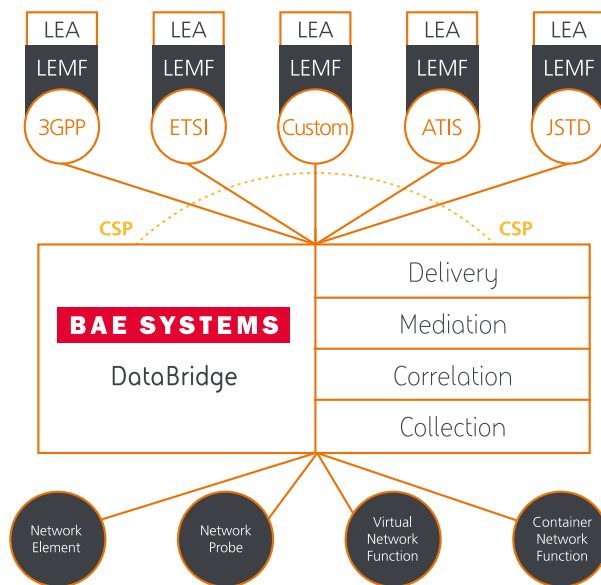


Figure 1: The DataBridge Lawful Intercept Solution

- **Cost efficiency** – Our standards-based, cloud native approach supports LI for all types of CSPs, from the largest global tier 1 carriers with more than 100 million subscribers, to new and growing CSPs.
- **Secure by design** – Built with security at its core, DataBridge is built and tested against the CIS and OWASP security standards.
- **Standards focused** – The DataBridge product team actively work with the 3GPP, ETSI and ATIS standards bodies to ensure that our solution and roadmap is always relevant and consistently complies with the latest standards revision.
- **5G Ready** – With existing production deployments, DataBridge fully supports LI on 5G Stand Alone (5GSA) networks.

DataBridge architecture

BAE Systems DataBridge is built around a highly scalable micro-service architecture that is aligned with the 3GPP standards LI model. This alignment with a standards based model, combined with our cloud native approach and our proven capability to support the latest 5G technology, streamlines and vastly simplifies delivery and integration of DataBridge into a CSP's network.

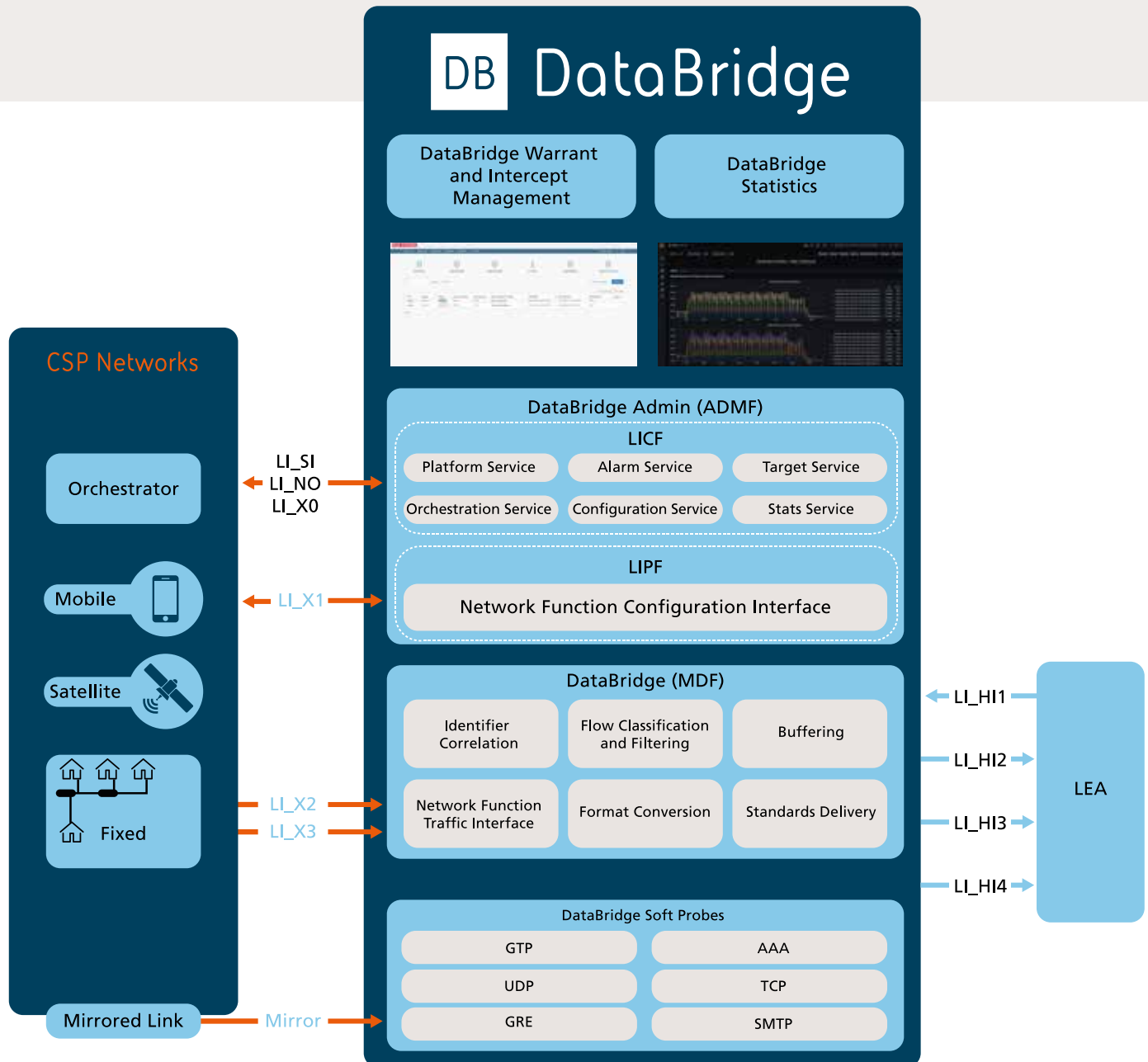


Figure 2: Architecture for BAE Systems DataBridge

Functionality and features

DataBridge is built on a cloud native micro-service based architecture, supporting VNF and CNF deployment models for voice and data interception on all types of fixed and mobile network, including full and proven integration with the latest 5GSA architectures. It provides the following features:

Flexible Warrant Management

The DataBridge Warrant Management System (WMS) simplifies the processes undertaken by an internal CSP compliance team tasked with supporting lawful access to communications data. The work carried out by this team is often the subject of strict processes, procedures and scrutiny. The DataBridge WMS provides CSPs with a modern and intuitive web based user interface designed specifically to meet the requirements of warrant data entry, authorisation, automated network provisioning, auditing and reporting.

DataBridge WMS can be deployed as part of a complete DataBridge LI solution or as a workflow tool, integrating with a CSP's existing LI infrastructure.



Figure 3: DataBridge Warrant Management UI

Cloud Native

DataBridge is designed and built from the ground up as a cloud native platform, enabling the freedom and flexibility to support the widest possible range of virtualisation technologies, and allowing us to align the solution with our customer's chosen technical direction.

Whether deployed as Container Network Functions (CNFs) within a public cloud like AWS, as Virtual Network Functions deployed on a private cloud such as ESXI, or deployed on dedicated COTS x86 hardware, DataBridge's cloud native architecture combined with our team's depth of experience will streamline and simplify deployment and integration.

Depending on technology choices and security paradigms, infrastructure requirements have always and will continue to vary between CSPs. In support of these differences, DataBridge has been developed as a platform agnostic solution, equally capable of running on dedicated COTS hardware, as VMs or containers within a cloud environment, with proven integration to a wide variety of cloud platforms and orchestration technologies.

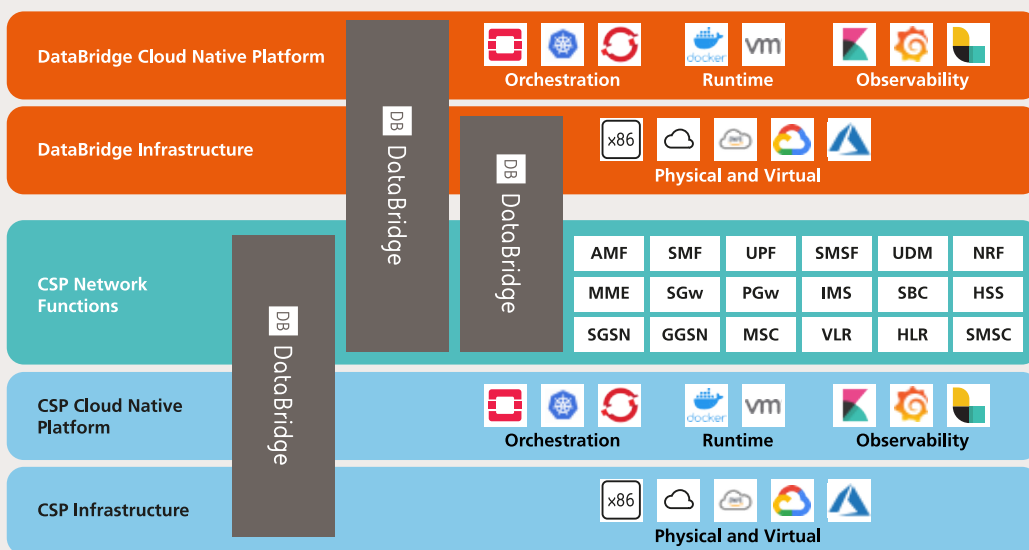


Figure 4: DataBridge deployment options

5G Identifier Association Function

As 5G Mobile architectures are deployed by CSPs, a benefit to users comes through significant enhancements to user privacy and security. This has been achieved through the introduction of Concealed and Temporary session based identifiers, which replace attributable and trackable identifiers as found on the 2G, 3G and 4G radio interfaces.

While these improvements are welcome from a User privacy perspective, providing protection against nefarious organisations and individuals, it makes the job of law enforcement much harder.

To address the gap in LEA capability introduced through these privacy protections, BAE Systems has developed and introduced the DataBridge 5G Identifier Association Function.

Based on the latest 5G LI 3GPP standards, the DataBridge 5G Identifier Association Function allows authorised agencies to attribute, in real time, observed 5G radio identifiers to a subscriber's permanent identifier.

The 5G Identifier Association Function can be deployed either as part of an existing DataBridge LI deployment or as a standalone capability alongside a CSP's or LEA's existing LI solution.

The DataBridge Identity Caching Function (ICF) provides high speed retention and retrieval for all AMF generated identifier association events within a 5G SA core. With support for over 150 million subscribers and a configurable cache retention period, the DataBridge ICF meets the needs of the world's largest Tier 1 operators within the most demanding regulatory environments.

The DataBridge Identifier Query Function (IQF) provides an interface for LEAs to request temporary and permanent identifiers for a 5G subscriber: this is done via the standards-based LI_HIQR interface, enabling both direct LEA access as well as local requests made through the DataBridge Warrant Management System (WMS) using the Identifier Association workflow.

High Speed Mediation

BAE Systems DataBridge is deployed at some of the world's largest Tier 1 fixed line and mobile operators, supporting ultra-high-speed services such as nationwide wholesale open access infrastructure, fibre-to-the-premises (FTTP) and multi-gigabit per second 5G mobile data services.

In support of these high-speed services, DataBridge offers up to 10Gbps of data mediation for a single intercept, with the total mediation capacity scalable on demand, ensuring mediation resource is always in excess of the inbound intercepted traffic rates.

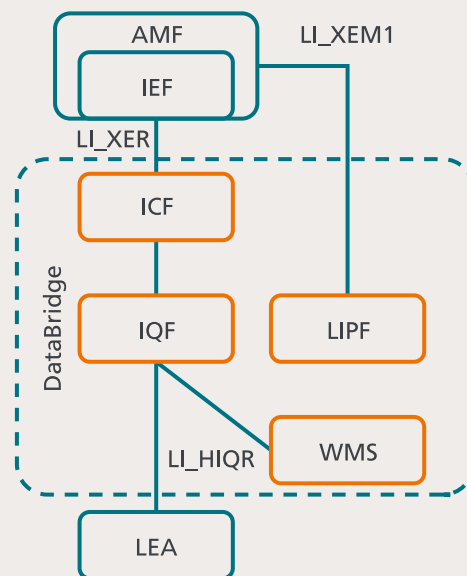
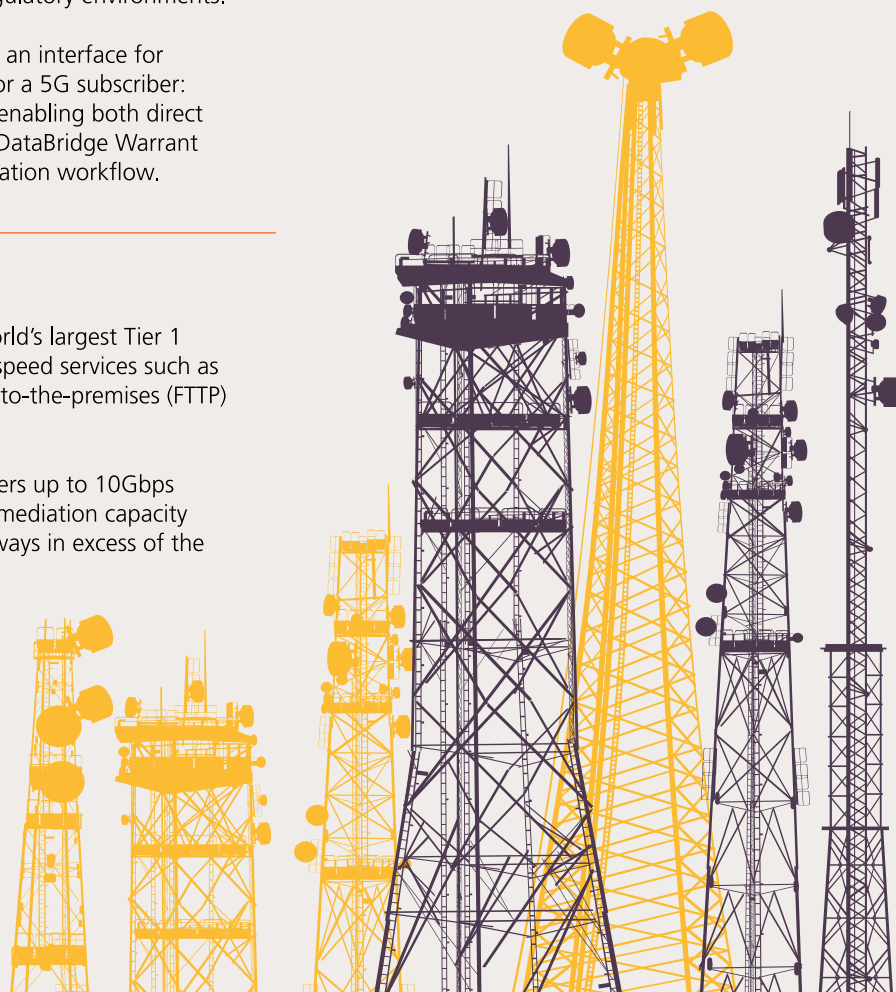


Figure 5: DataBridge 5G Identifier Association Architecture



Content Filtering

Whether it's FTTP fixed line services or 5G Mobile services, the bandwidth available to subscribers is ever increasing. While DataBridge has and will continue to support high-rate mediation and delivery in line with our customers high-speed service offerings, in some circumstances agencies request that CSPs reduce the delivery rates by removing specific low-intelligence value traffic types, such as high-rate video streaming services (e.g. YouTube).

In support of this requirement, DataBridge offers a fully integrated content filtering capability which can be invoked on either a global or per warrant basis. This capability supports law enforcement by performing granular traffic reduction at a per warrant and protocol level, while continuing to generate metadata about the filtered content flows.

DataBridge Content Filter can be enabled in any DataBridge deployment, but can also be deployed at the boundary between the CSP and the LEAs as a stand-alone function without modification to existing LI capabilities.

DataBridge content filtering enables traffic filtering and redaction on a per intercept basis with options to generate and deliver metadata (H12) for filtered flows.

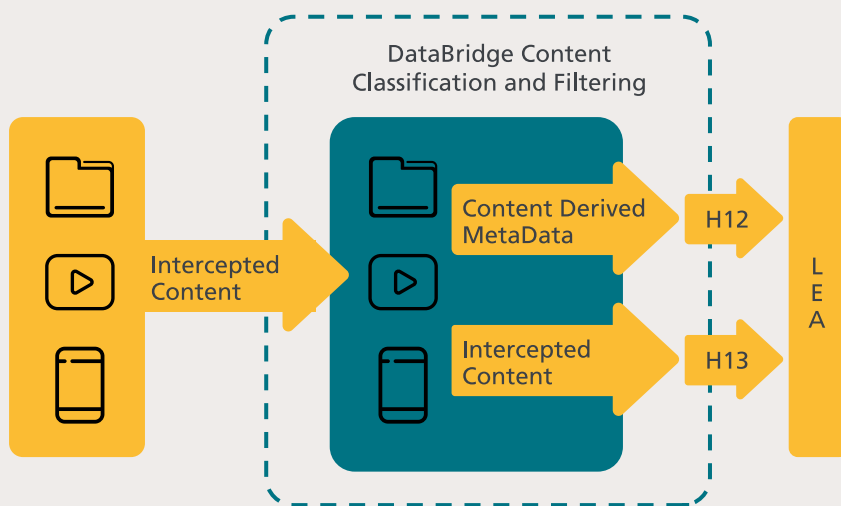
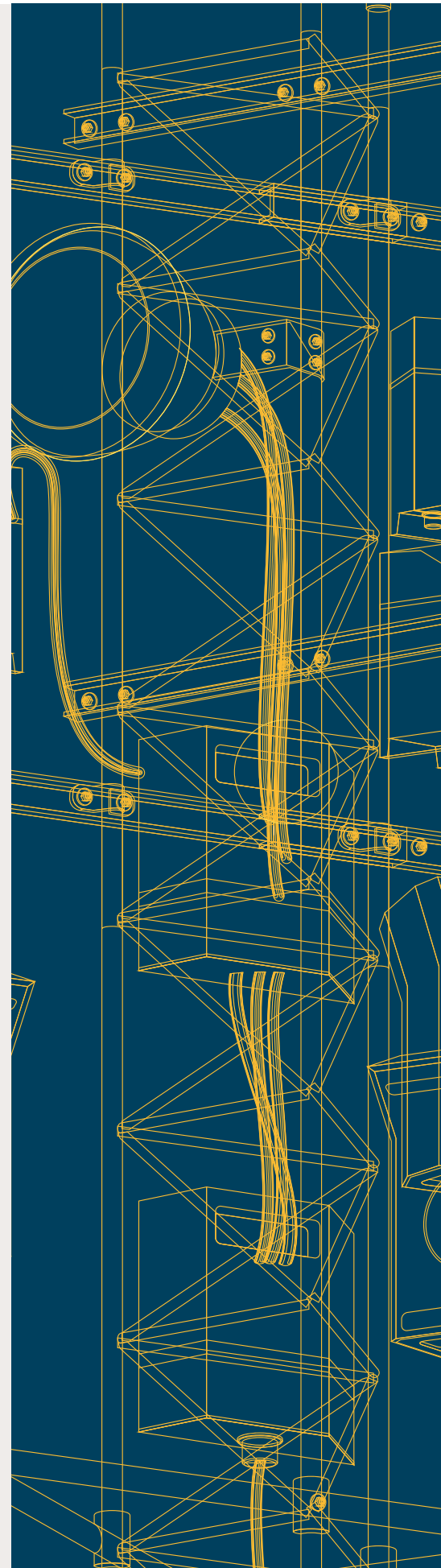


Figure 6: DataBridge Content Classification and Filtering



Advanced System Monitoring

A key part of any LI solution is the provision of a monitoring function that demonstrates clearly to regulators and law enforcement agencies that a CSP is meeting their regulatory obligations.

This monitoring functionality should provide a highly-granular historic and real time view of all the intercepted traffic that is requested, received and delivered to law enforcement by the CSP's LI solution.

The BAE Systems DataBridge advance system monitoring function (DBStats) supports CSPs in this requirement by providing a holistic view of system performance across the entire LI platform, covering every byte of data that is received, processed and delivered.

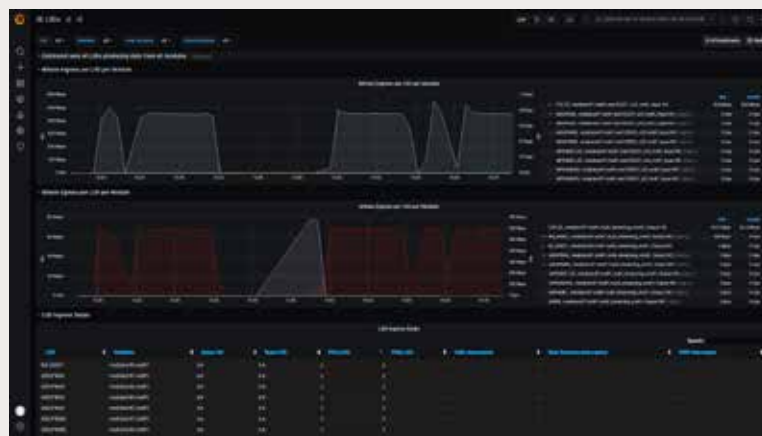
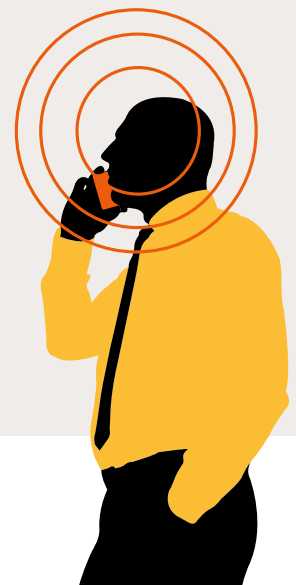


Figure 7: DBStats dashboards



Network Probes

While the majority of LI can be performed in partnership with LI interfaces imbedded within the Network Functions, there are some scenarios where intercepting traffic directly from the transport network is more cost effective or appropriate.

In support of these use cases, DataBridge 1G, 10G or 100G cloud native software-based probes can be deployed to provide intercept capability for the following use cases:

- IP voice interception with SIP and RTP protocols
- IP data interception on fixed and mobile networks
- Roaming IP Data on the S8 and N9 interfaces of a mobile network
- Home routed IP voice carried over the S8 (S8HR) or N9 (N9HR) interfaces
- Access to RADIUS and DHCP session information

Enhanced Location

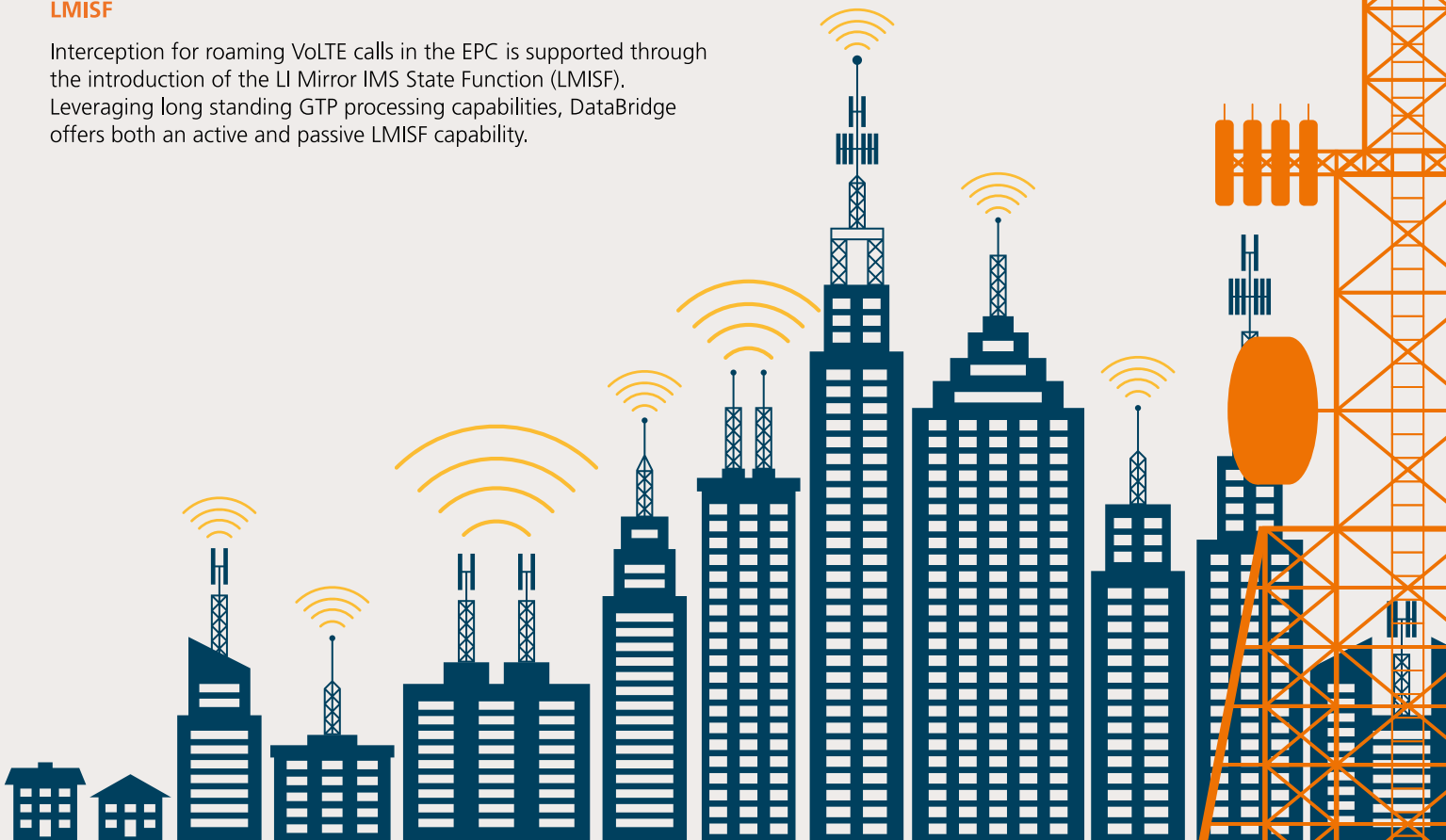
The Enhanced Location capability within DataBridge is a passive solution for providing high accuracy location information for all subscribers all the time, including building level, x & y axis coordinate information, as well as z axis for 5G, for all subscribers whether in active or idle mode.

SX3LIF

Control and User Plane Separation (CUPS) for the Evolved Packet Core (EPC) introduces the Split X3 Lawful Intercept Function (SX3LIF). Where the SX3LIF is not available within the CSP's network functions, DataBridge can provide this as an external capability.

LMISF

Interception for roaming VoLTE calls in the EPC is supported through the introduction of the LI Mirror IMS State Function (LMISF). Leveraging long standing GTP processing capabilities, DataBridge offers both an active and passive LMISF capability.



Technical Specifications

Network Equipment Vendor Support

- Broadsoft
- CASA Systems
- Cisco
- DriveNets
- Ericsson
- Huawei
- Juniper
- Mavenir
- Affirmed
- Microsoft
- HPE
- Mitel
- Nokia
- Oracle
- Packet Cable
- Redback
- Ribbon
- Samsung

Supported Network Technologies and Services

Fixed line

- DSL – Voice and Data, Email (POP3, SMTP, IMAP, webmail)
- Cable Voice and Data, Email (POP3, SMTP, IMAP, webmail)
- PSTN voice

Radio Access

- GPRS – Voice, SMS, MME, Internet Access
- GSM – Voice, SMS, MMS, Internet Access
- UMTS – Voice, SMS, MMS and Internet Access
- LTE – Voice, SMS, Internet Access and IMS/RCS
- 5G – Voice, SMS, Internet Access
- Satellite Voice and Internet Access

Network Probe Interface Support

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

Standards Compliance

- TIA J-STD-025-A
- TIA J-STD-025-B
- ATIS 10000678
- ATIS 1000013.2007
- 3GPP 33.106-108
- 3GPP 33.126-128
- ETSI 201.671 – TDM Voice
- ETSI 101.671 – VoIP
- ETSI 102.232 parts 1-7
- ETSI 103 221-1
- ETSI 103 221-2
- ETSI 103 120

Platform 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

Deployment Options:

- DataBridge Cloud Deployment (CSP Private, Public, DataBridge Private) – Support for Containers and VMs with integration into a choice of Management and Orchestration technologies
- DataBridge supported Cloud technologies – OpenStack, VMWare, AWS, Kubernetes, OpenShift, Azure, Google Cloud
- DataBridge hosted on physical COTS Hardware

For further details of BAE Systems DataBridge, please contact us.





We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

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

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 290 539 330

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +44 (0) 330 158 3627

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6951 2440

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

E: learn@baesystems.com

W: baesystems.com/digital

 [linkedin.com/company/baesystemsdigital](https://www.linkedin.com/company/baesystemsdigital)

 twitter.com/BAES_digital

Copyright © BAE Systems plc 2023. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc.

BAE Systems Digital Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ.

No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Digital Intelligence.

BAE SYSTEMS