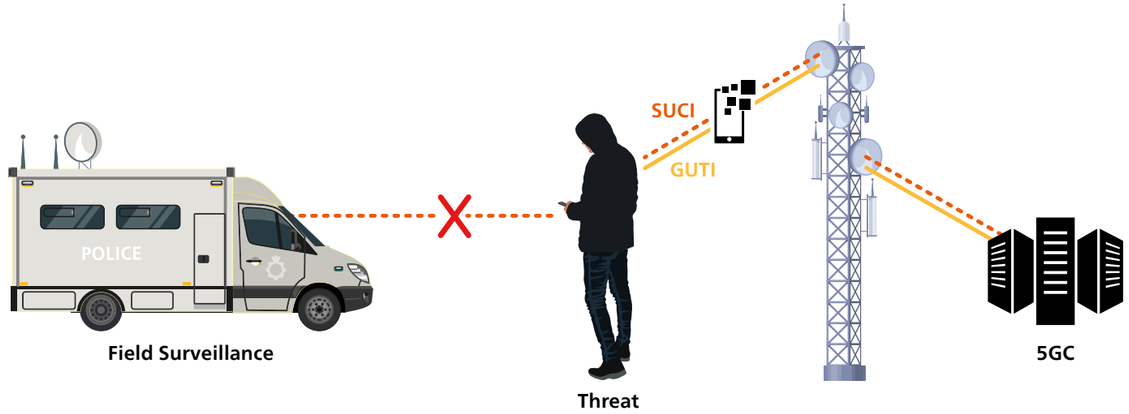
DataBridge^{7} 5ID

Digital Intelligence

BAE SYSTEMS

5G Identity De-concealment

One of the key advantages of Fifth Generation (5G) mobile technology is the introduction of significantly enhanced privacy protections for subscribers. These security advances include the removal of permanent subscriber identifiers from exposure on the radio interface. Where 4G networks still expose a subscriber's IMSI and traceable T-IMSIs, 5G replaces these identifiers with ephemeral and encrypted alternatives to ensure that attribution of subscribers to observable identifiers is no longer possible. These advances deliver clear benefits to consumers, enterprises and governments alike - but they also fundamentally change the operational environment for lawful investigation.



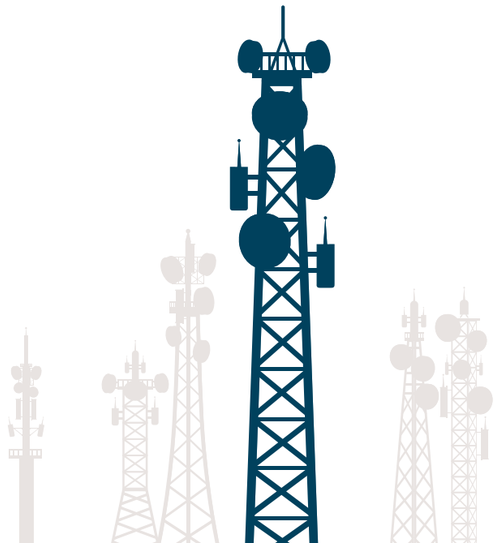
Traditional Cell Site Simulation meets 5G reality

For many years, law enforcement agencies have relied on Cell Site Simulation and IMSI-based techniques to identify devices of interest within a geographic area. These techniques were developed at a time when CSPs exposed stable identifiers more readily and when correlation between radio-observed identifiers and real subscribers was comparatively straightforward. In 5G networks, this assumption no longer holds because:

- Permanent identifiers are cryptographically protected and never broadcast
- Temporary identifiers change more frequently and are scoped more tightly
- Authentication and identity handling are deeply embedded in the core network
- Rogue or simulated base stations are far more difficult to use effectively

As a result, traditional equipment has become incompatible with 5G environments. The very privacy and security features that make 5G resilient against fraud, surveillance and identity theft also mean that legacy investigative techniques must evolve.

Following the roll out of 5GNSA and 5GSA alongside 4G LTE networks, traditional IMSI-based surveillance techniques can still be deployed. But, as CSPs transition to a fully all-5G network and legacy technologies are retired, these traditional techniques and equipment will become either profoundly affected or completely obsolete.



ETSI provides a way forward: Understanding ICF and IQF

The European Technical Standards Institute (ETSI) provides a framework for overcoming the challenges 5GSA brings to traditional IMSI-based techniques. ETSI defines the following functions which enable resolution of temporary identifiers to permanent subscriber identity:

- **IEF:** Identity Event Function is a network element that tracks temporary subscriber identifier changes in the network and provides then as records to the Identity Caching Function (ICF). If it exists within the 5G network, the IEF manifests as a 'sub-function' located within the 5G core Access and Mobility Management Function (AMF).
- **ICF:** Identity Caching Function ingests association record events from the IEF and caches them so that they can be later queried by Law Enforcement when required.
- **IQF:** Identity Query Function is responsible for handling LEA queries for identity associations and interfacing with the ICF to obtain and deliver the correct association mapping for individual queries.

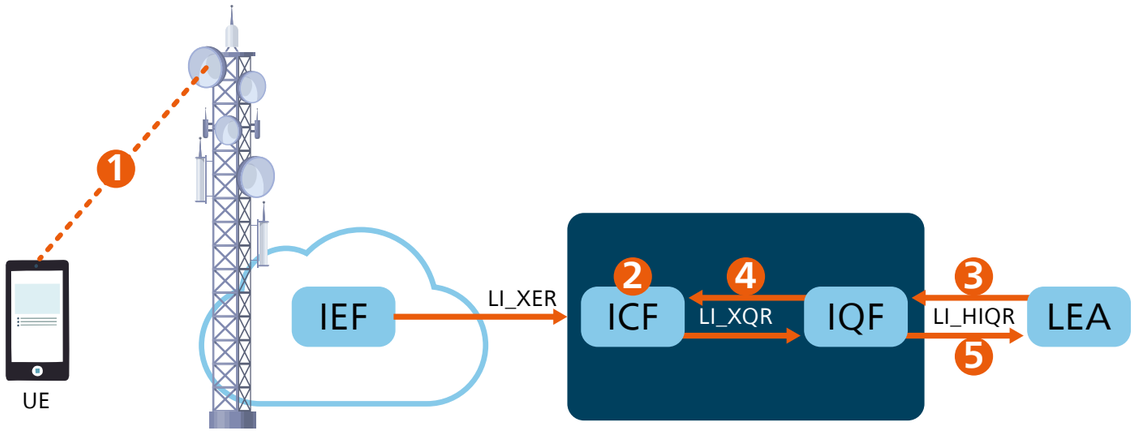


Figure 1: *ICF/IQF event/request/response lifecycle*

The ICF and IQF work together to implement a cached identifier mapping service that provides law enforcement with a mechanism to translate temporary identifiers into meaningful subscriber identities using a standardised interface and workflow. Generally the workflow is as follows:

1 **Association/de-association events:** The UE (User Equipment) undergoes a network event in which the network generates identity association events (temporary <> permanent mappings) which are sent from the IEF to the ICF.

2 **Caching:** The ICF maintains these mappings for a configurable period.

3 **LEA query:** The LEA generates a query (e.g. “What permanent ID corresponds to this temporary identifier observed at time T?”) and sends it to the IQF.

4 **Lookup:** The IQF validates and forwards the query to the ICF.

5 **Response:** The ICF returns matching mappings to the IQF, which then returns them to the LEA.

BAE Systems provides the solution: 5G Identity De-concealer (5ID)

Implementing ETSI ICF and IQF

Where 5G de-concealment is required, DataBridge⁷ 5ID provides an integrated ICF and IQF solution designed to meet the requirement blueprint as directed by ETSI for permanent/temporary identifier de-concealment within the 5G domain. It enables CSPs to reliably capture, cache and resolve associations between permanent subscriber identities and dynamic network identifiers, delivering fast and accurate identity resolution. By keeping in close lockstep with identifier association events from across the network and securely caching them for LEA query, DataBridge⁷ 5ID ensures that critical identity relationships are accurately, securely and reliably preserved for LEA obtainment and utilisation.

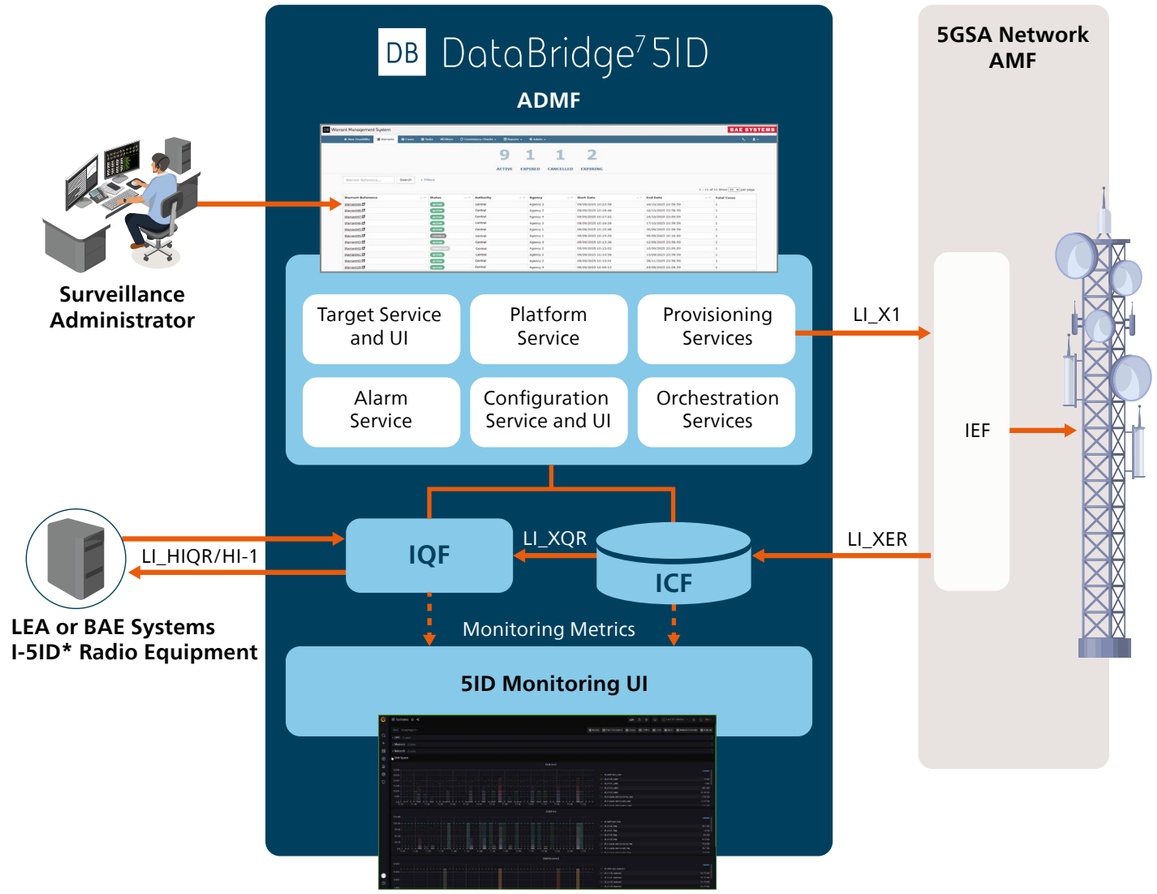


Figure 2: *DataBridge⁷ 5G Identity De-concealer (5ID) architecture*

* BAE Systems Integrated 5G Identity De-concealer (I-5ID) provides the cell-site simulator radio piece for the end to end de-concealment lifecycle.

Core ADMF services

DataBridge[7] 5ID provides core ADMF services that include:

- **Full integration with the DataBridge7 -** product supporting all standard platform management, configuration and orchestration services (e.g. monitoring, logging, alarms, access controls etc).
- **Target Service and UI -** provides a complete and flexible warranty administration via machine-to-machine interface or web based user-interface.
- **Provisioning Services -** software modules that support IEF LI_X1 Management.

Surveillance administration of DataBridge[7] 5ID

DataBridge[7] 5ID can exist standalone or in parallel with an existing DataBridge[7] LI platform. Administration of DataBridge[7] 5ID may be performed using the following methods:

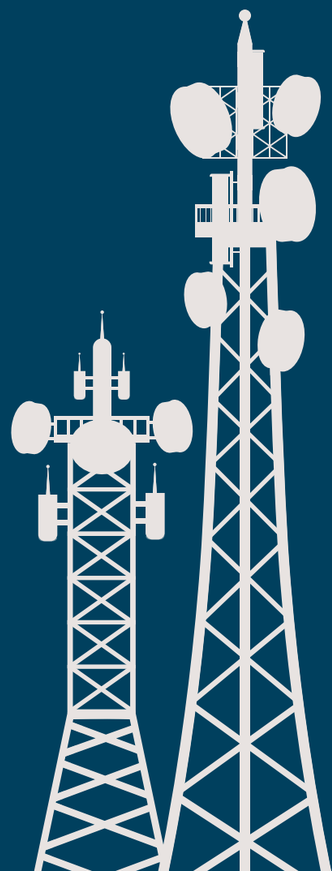
- ETSI TS 103.120 HI-1 eWarrantry service - ETSIs directed method of IQF interaction. DataBridge[7] 5ID is fully compliant with ETSI TS 103.120 in the ICF/IQF context, enabling LEAs to manage IQF requests with the use of LDTaskObject Request Objects and responses in the form of IdentityAssociationRecord Delivery Objects in conjunction with any customised workflow that utilises standardised HI-1 defined objects.
- DataBridge[7] WMS (Warrant Management System) - provides a secure, flexible and intuitive web UI platform for de-concealment surveillance type administration that is specifically designed to meet the requirements of warrant data entry, authorisation, automated network provisioning, auditing and reporting.

In addition to the above surveillance administration workflows, DataBridge[7] 5ID includes DataBridge[7] Architect, an intuitive web UI platform purposed with environment setup and configuration management of all system and software modules. In the context of the de-concealment and disclosure domain, relevant configuration includes ICF retention period definition, IEF source input configuration, IQF security settings and more.

5ID monitoring - DBStats

DataBridge[7] DBStats provides real-time and retained granular statistics to keep system operators informed of all 5ID and LI activity over a desired period range. DataBridge[7] DBStats provides the following ICF/IQF statistics and visualisations:

- Real-time current and historical ICF cached identity association record count
- Graphical view of received identity association record updates against time per surveillance and total
- ICF LI_XER ingest function volumetrics including input rates (pps and bitrate), dropped packets and malformed input data count
- ICF database storage retention and storage utilisation
- IQF client request log and count
- ICF and IQF software module compute and memory utilisation



Passive approach - DataBridge[7] IEF Probe

Where a 5GSA core does not provide access to an IEF function at the AMF, or a passive approach is preferred, subscriber identity de-concealment may be performed using a non-ETSI standardised approach with the use of DataBridge[7] IEF Probe.

DataBridge[7] IEF Probe executes the function of an IEF by passively ingesting control events transmitted on 5GSA N1/2, N11, N12 and N13 interfaces and generating IEF-like association/de-association events in the process. All subscriber association/de-association and session metadata is processed by IEF Probe and exposed to ICF-clients using either ETSI standardised LI_XER event messages or proprietary event messages that contain additional metadata acquired from the N1/2, N11, N12 and N13 5GSA interfaces.

DataBridge[7] IEF Probe is capable of delivering to a third party ICF/IQF solution or can be deployed in conjunction with DataBridge[7] 5ID.

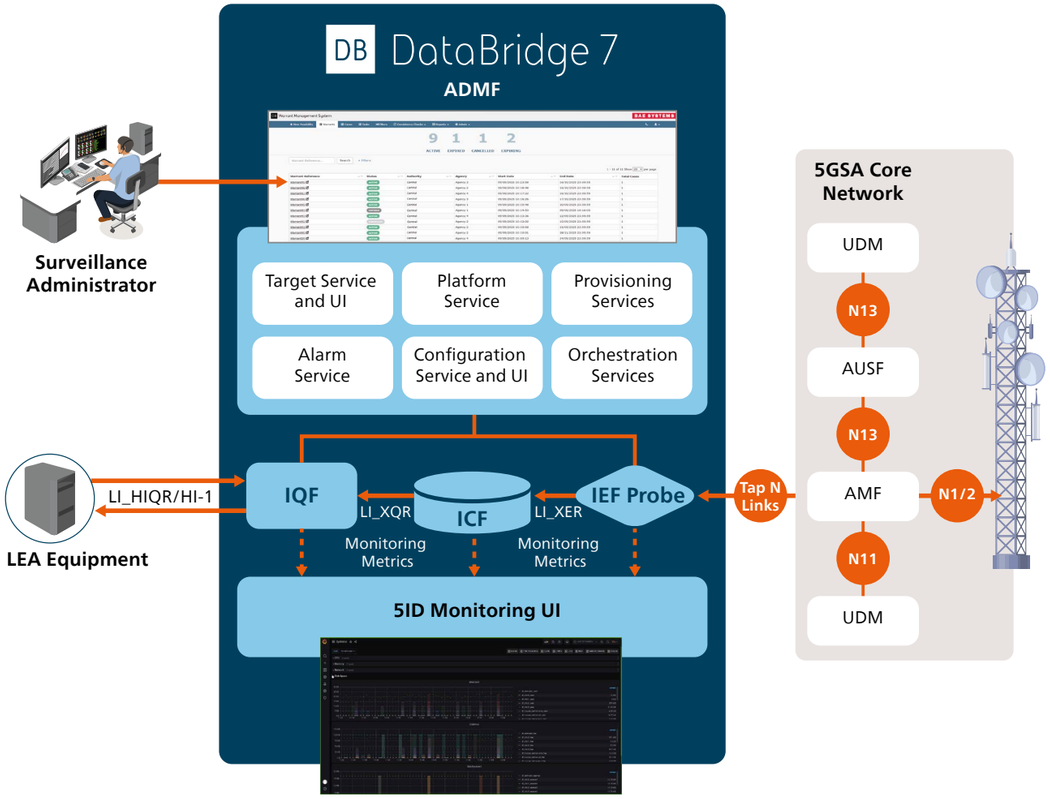


Figure 3: *DataBridge7 5G Identity De-concealer (5ID) with IEF Probe*

Supported interfaces

- **LI_HIQR/HI1, LI_XQR, LI_XER -** compliant with ICF/IQF related and ETSI TS 133.128 defined interfaces
- **LI_X1 -** compliant with ETSI TS 103 221-1

We are Digital Intelligence

Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared.

Our teams provide advanced digital capability, products and solutions that weave together digital threads of data so that customers get the vital insight they need – from the fine detail to the bigger picture, providing the power of perspective to confidently make the critical decisions that keep our societies safe and able to thrive.

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. Whether on land, in the air, at sea, in space or cyberspace, we're your digital mission partner, with you every step of the journey.

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

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS