DataBridge[7] HI-1 eWarrantry

Digital Intelligence

BAE SYSTEMS

HI-1 Processes Were Never Meant to Scale

Lawful Interception (LI) and Lawful Disclosure (LD) obligations are growing in volume, urgency and complexity. Yet for many organisations, the HI-**1** warrant handling process still relies on approaches that were designed for a far smaller, slower and less regulated world.

Without a true machine-to-machine interface, HI-**1** processes typically depend on email, PDFs, spreadsheets, ticketing systems, or ad-hoc portals.

These approaches introduce significant challenges:

- **Operational inefficiency:** Manual handling of warrants increases processing time, especially as request volumes rise.
- **Human error risk:** Re-keying data, misinterpreting scope, or missing updates can lead to costly mistakes.
- **Poor traceability:** Auditing who received, processed, acknowledged, or acted on a warrant becomes difficult and time-consuming.
- **Inconsistent execution:** Different teams or individuals may interpret and implement requests differently.
- **Delayed compliance:** Time-critical requests suffer when workflows rely on human availability rather than automated processing.

The pitfalls of proprietary API use

In an environment where accuracy, timeliness and accountability are critical, manual HI-1 handling is increasingly unsustainable.

Recognising these issues, some countries and LEAs have introduced custom or proprietary APIs to automate warrant exchange. While this is a step forward, it typically introduces a new set of problems:

- **Vendor lock-in:** Each proprietary interface ties customers and partners to a specific implementation.
- **One-off integrations:** Every law enforcement agency or service provider requires bespoke development, testing and maintenance.
- **Inconsistent semantics:** The same LI concept may be represented differently across APIs, increasing the risk of misinterpretation.
- **High change costs:** Regulatory or process changes require coordinated updates across multiple bespoke interfaces.
- **Limited interoperability:** Cross-border or multi-vendor environments can become complex and fragile.

Instead of simplifying HI-1, proprietary APIs often shift complexity from the operations space to the engineering realm, failing to realise the intended benefit.

Additional challenges often overlooked

Beyond efficiency and interoperability, organisations also struggle with:

- **Audit and compliance readiness:** Demonstrating end-to-end compliance to regulators or courts.
- **Lifecycle management:** Handling modifications, renewals, suspensions and expirations of warrants in a controlled way.
- **Security and integrity:** Ensuring warrants are genuine, authorised and processed only by approved systems.
- **Future scalability:** Preparing for increasing automation, cross-jurisdiction cooperation and evolving Lawful Interception frameworks.

These challenges demand more than automation — they demand standardisation.

Standards-based HI-1 eWarrantry with ETSI TS 103.120

ETSI TS 103.120 provides the foundation for a standards-based, interoperable, machine-to-machine HI-1 interface specifically designed to address the operational and technical challenges of warrant handling. Rather than defining yet another bespoke integration, ETSI TS 103 120 establishes a common language, structure and process for exchanging warrant and tasking information between law enforcement authorities and service providers. By adopting ETSI TS 103 120, organisations can move from ad-hoc or proprietary approaches to a repeatable, scalable and terminology aligned HI-1 model.

ETSI TS 103 120 defines a machine-to-machine interface for the structured exchange of warrant and tasking information, providing a common data model and shared semantics that ensure consistent interpretation across systems. The specification supports the full warrant lifecycle - from submission and acknowledgement through modification, suspension and termination - while enabling secure, authenticated and integrity-protected communication between authorised parties. By promoting interoperability across vendors, service providers and jurisdictions, ETSI TS 103 120 reduces integration complexity and avoids proprietary lock-in, while its structured messaging supports traceability, audit, compliance and accountability. Designed to accommodate national profiles and regulatory variation, the standard delivers a future-proof, extensible foundation for scalable, compliant and automation-ready HI-1 processes.

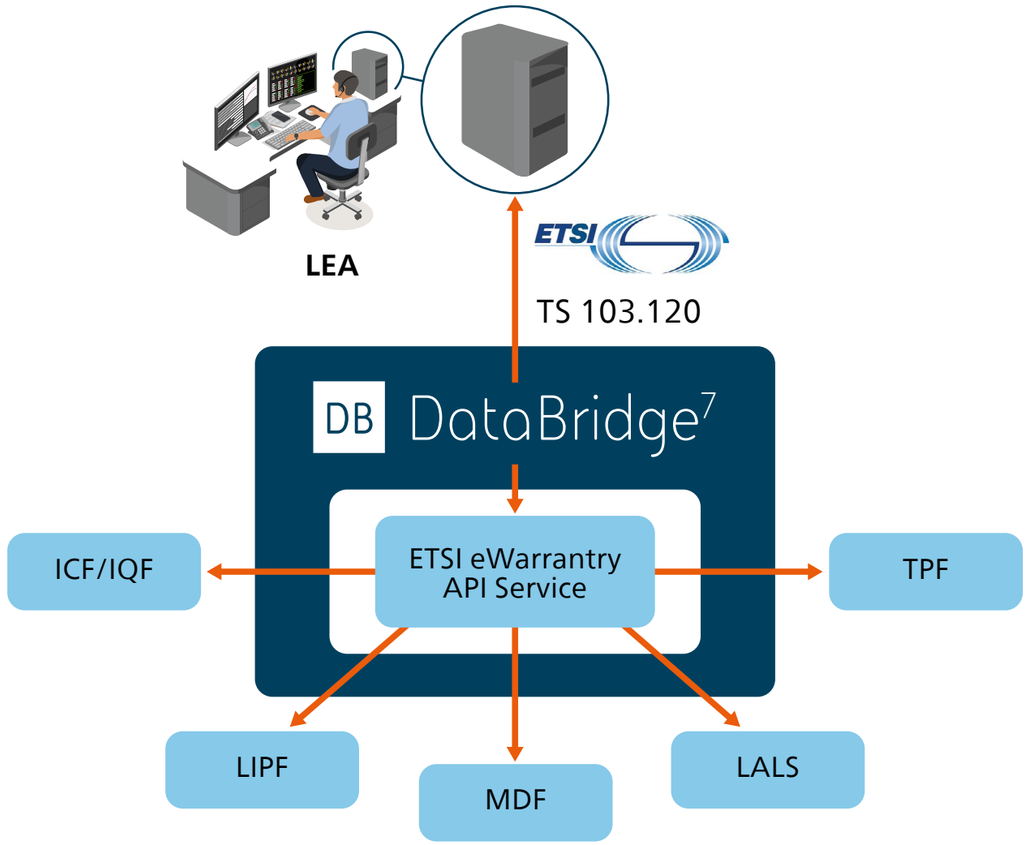
DataBridge^7 ETSI eWarrantry

Where eWarrantry is required, DataBridge^7 delivers a ready-to-deploy, productised implementation of ETSI TS 103.120 - transforming the standard from a specification into an operational HI-1 capability. It removes the burden of designing, building and maintaining a compliant interface, allowing organisations to adopt a standards-based HI-1 model quickly and with confidence. It encapsulates the complexity of the ETSI specification within a stable, well-defined API, handling protocol logic, validation, state management and error handling out of the box. It supports the complete warrant lifecycle - submission, acknowledgement, modification, suspension and termination - while maintaining full traceability and audit readiness.

By natively implementing the ETSI TS 103 120 data models, message flows and lifecycle semantics, DataBridge^7 provides a fully compliant HI-1 interface that integrates seamlessly into existing lawful interception and disclosure environments. This ensures consistent interpretation of warrants, automated processing and reliable execution across both internal systems and external partners.

Workflow and National Profiles

Although the definition of HI-1 objects are standardised through ETSI, each organisational and national use of the ETSI TS 103 120 HI-1 interface will follow locally established processes and workflow rules. As such, DataBridge^7 ETSI eWarrantry does not provide a rigid workflow out of the box or a 'one-size-fits-all' product, but a configurable and flexible solution that accommodates existing and established local and operational workflows. Further to this, DataBridge^7 ETSI eWarrantry is designed to incorporate new and developing workflow profiles and national profiles for organisations implementing ETSI TS 103.120 for the first time. We offer consultancy expertise to accelerate business process integration in order to expedite deployment and operational readiness.



In short, DataBridge^7 doesn't just implement the ETSI TS 103.120 standard - it adapts to local Lawful Interception and Disclosure frameworks. Organisations can standardise data exchange, enforce compliance and maintain traceability, while still maintaining and upholding the nuances of local operational workflows.

Core Objects and Data Definitions

DataBridge^7 ETSI eWarrantry supports management of the following key workflow attributes:

- **Authorisation:** A fundamental element to the security of the warrant lifecycle. Through the use of TS 103.120 AuthorisationObjects within the workflow lifecycle, DataBridge^7 ETSI eWarrantry ensures that all tasking is correctly and securely approved and authorised by the appropriate Law Enforcement authorities. DataBridge^7 ETSI eWarrantry ensures that every operation is transparently linked to an active, approved authorisation. This provides clarity for operators, confidence for compliance teams, and assurance for auditors and regulators.
- **Documentation:** TS 103.120 defines DocumentObjects which represent structured, self-contained records of legal and operational documents such as warrants, authorisations, amendments and supporting material each with clearly defined metadata, lifecycle states and relationships. By adopting DocumentObject management, DataBridge^7 ETSI eWarrantry enforces clarity, control and confidence at the heart of warrant processing workflows.
- **Notification:** DataBridge^7 ETSI eWarrantry leverages ETSI TS 103 120 NotificationObjects to deliver structured, reliable and auditable communication of events and status changes across the warrant-processing lifecycle. NotificationObjects ensure that all parties share a common understanding of what has happened, when it happened, and which warrant artefacts are affected.

Base LI Tasking - LIPF and MDF

DataBridge[7] ETSI eWarrantry is designed for the Lawful Interception (LI) domain and is fully compliant with the use of ETSI 103.120 LITaskObjects. LITaskObjects are central to ETSI's Lawful Interception framework. They formally define the tasks that must be carried out to fulfil a lawful request - such as initiating, modifying, suspending, or terminating interception activities - while maintaining a clear linkage to the underlying authorisations and documentation. The provisioning of ETSI LITaskObjects within the implemented workflow enables DataBridge[7] to automate and execute all POI tasking, data mediation and data delivery to LEMFs.

With ETSI-compliant LITaskObjects, DataBridge[7] ETSI eWarrantry enables:

- Explicit task modelling, aligned with lawful interception operations and responsibilities
- Clear linkage between tasks, authorisations and documents to support end-to-end traceability
- Lifecycle control covering task creation, activation, modification, suspension and termination
- Audit-ready operations, with structured records suitable for oversight and regulatory review

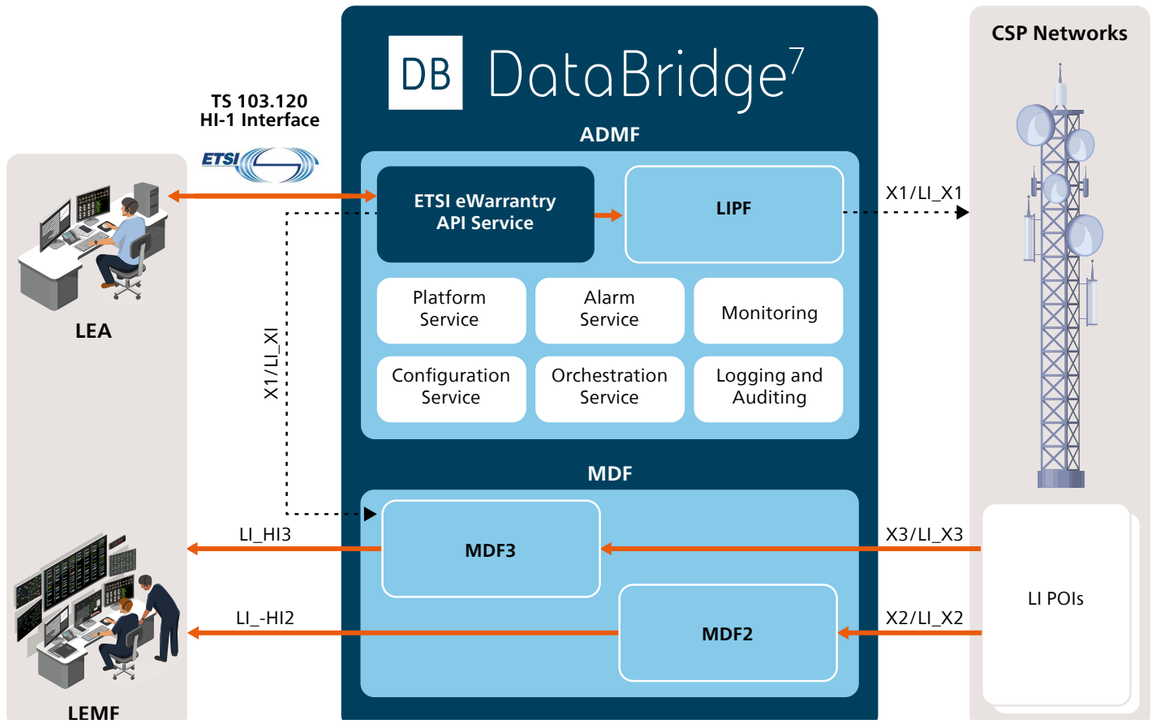


Figure 1: *ETSI HI-1 administration of DataBridge[7]*

Traffic Policies and Traffic Rules

In addition to core LI capability, DataBridge[7] ETSI eWarrantry supports utilisation of Traffic Policies that can be enforced upon intercepted materials correlated and referenced by an LITaskObject. ETSI TS 103.120 provides standardised objects and direction that enables LEAs to content select delivery of intercepted X3/HI3 traffic using configurable criteria provisioned within TrafficPolicyObjects and TrafficRuleObjects. DataBridge[7] ETSI eWarrantry enables LEAs to create and manage TrafficPolicyObjects and TrafficRuleObjects in compliance with standardised behaviours as per the ETSI TS 103.120 specification. DataBridge[7] ETSI eWarrantry Traffic Policy capability operates alongside DataBridge[7] Traffic Policy Function (TPF), which provides the data-plane processing capability of Traffic Policy Object application to the intercepted traffic.

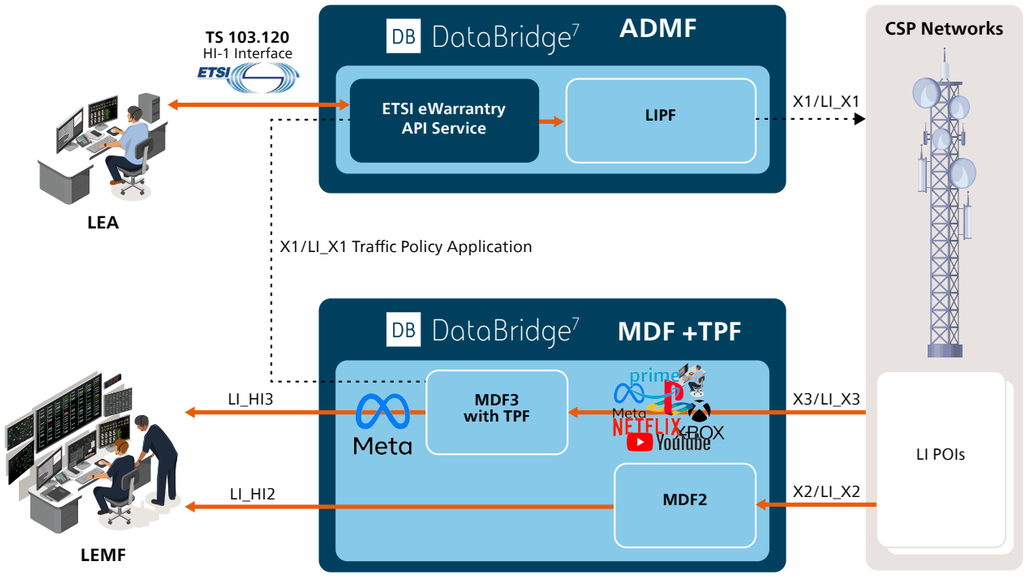


Figure 2: *ETSI HI-1 administration of combined DataBridge[7] with Traffic Policy Function (TPF)*

Lawful Disclosure Domain - ICF/IQF

Where 5GSA Temporary Identifier De-concealment is required, DataBridge[7] ETSI eWarrantry is fully compliant with the IQF Lawful Disclosure (LD) LI_HIQR interface as directed by ETSI TS 133.128 and ETSI TS 103.120. DataBridge[7] ETSI eWarrantry supports:

- LDTaskObject Requests pertaining to the LI_HIQR Request definition as per ETSI TS 133.128.
- Asymmetrical responses delivered as a DELIVER Request in the form of an ETSI TS 103.120 DeliveryObject. Responses are defined in accordance with IdentityAssociationRecords as per ETSI TS 133.128.

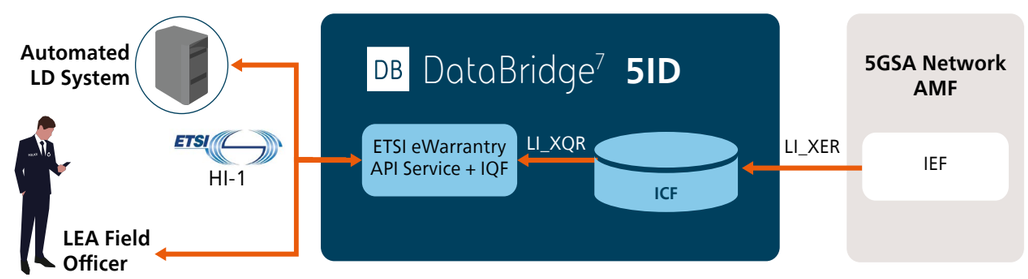
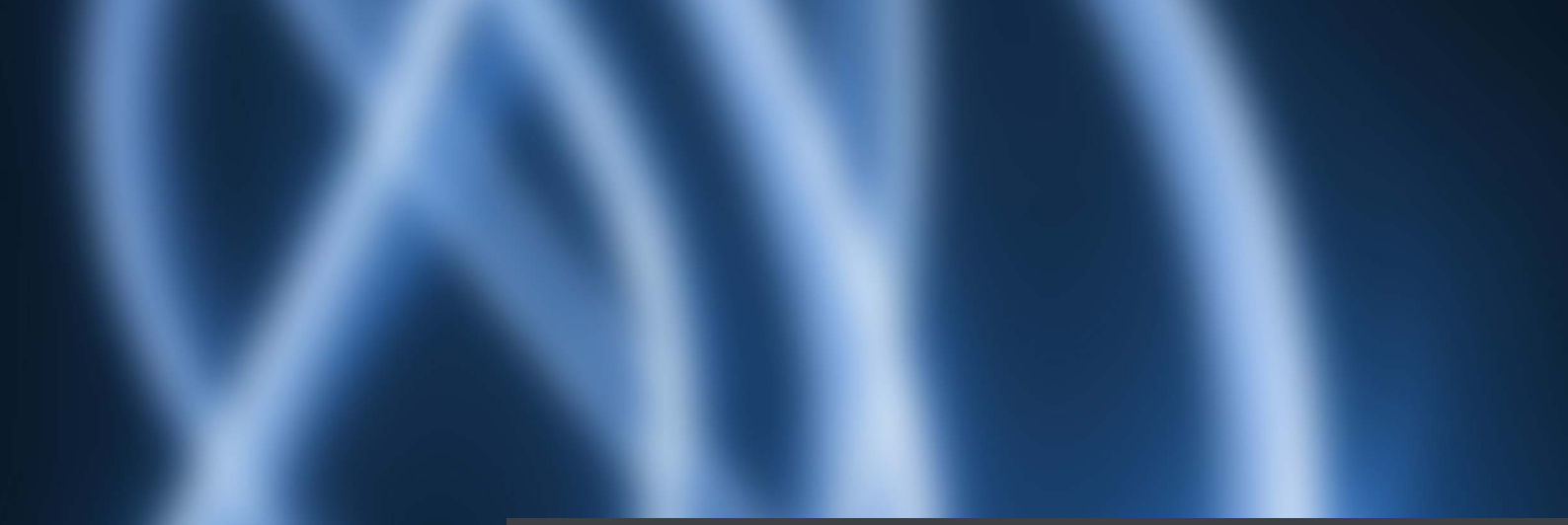


Figure 3: *ETSI HI-1 administration of DataBridge[7] 5ID*



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