



2iC TRUST (Deployed use) for MOD open standard Lean Services Architecture (LSA) - Services Definition

Date:	Wednesday, 28 January 2026
Version:	202601-28-1
Author(s):	Tom Berry
Status:	FINAL

Confidentiality

This document is commercially sensitive and remains the property of 2iC Limited.

2iC Limited, registered in England and Wales number 07183164

2 Venture Road, Southampton Science Park, Chilworth, Southampton, SO16 7NP, UK

P: +44 (0) 208 123 7479

www.2iCworld.com

E: info@2iCworld.com



▪ 2iC TRUST for Deployed Use

2iC TRUST is commercial-off-the-shelf (COTS) cross-domain software that delivers assured digital interoperability between devices, systems and networks across different trust domains. These differing trust domains can be defined by different security classifications or different boundaries where there is a need to separate systems, information and equipment.

2iC TRUST is typically provided as a package with a trusted hardware supplier. Please contact 2iC or our partners for more details.

1. 2iC TRUST

2iC TRUST software has successfully operated on various cross-domain hardware platforms. From small, soldier- worn wearables to rack-mounted equipment. This provides unique flexibility, adaptability and speed of implementation for cross-domain solutions to the Warfighter.

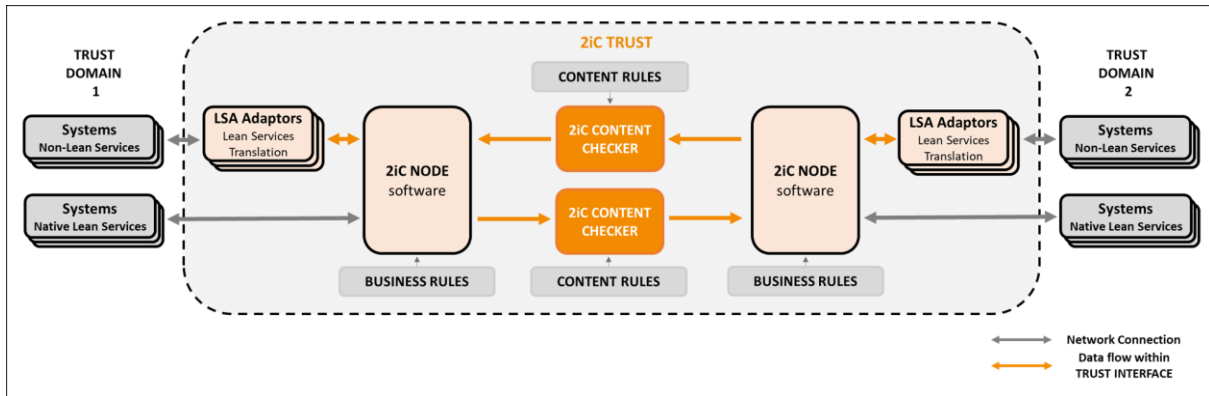
Whether on land, sea or air, defence forces and suppliers worldwide need to rapidly implement secure and free-flowing digital interoperability between different devices from different manufacturers—legacy, current and future—using numerous interfaces and protocols.

2iC TRUST enables secure cross-domain interoperability by delivering the following key benefits:

- Accelerates information throughput and data integrity by negating the need for humans to manually transport, translate or screen the data at each trust boundary.
- Introduces a protocol break meaning only predefined data types are permitted to cross the trust boundary, preventing the ingestion of unexpected data and drastically reducing the number of cyberattack vectors that a system is open to.
- Granular content checking functionality allows the screening of data payloads before they cross the trust boundary, ensuring that they fall within expected tolerances and prevents unauthorised data from entering or leaving a trust domain.
- Allows the seamless integration of almost all legacy, current and future devices by taking advantage of a Modular Open Systems Approach (MOSA).
- Negates the need for duplicated software systems in different domains and so reduces complexity and cost.
- Integrates securely with systems with restricted access such as export restrictions or higher security classifications.

○ 2.1 2iC TRUST technical overview

- The following diagram shows how 2iC TRUST controls the flow of shared data.



- 2iC TRUST software works with flow control that can either be hardware or software enforced, depending on the security requirement. Business rules manage the integration with systems in each of the domains and the content rules define fine-grained content checks around what ranges and types of data are permitted to pass through.
- Both business and content rules are created using 2iC DESIGNER. These reconfigurable rules define what information can pass and what is being checked. The software's built-in Content Checkers implement the open standard Barrier Validation Rules as defined in the LSA Specification to prevent unauthorised data from leaving or entering a trust domain.
- As the 2iC TRUST software is platform (hardware or software) agnostic it can adapt to provide cross-domain security in almost any operational scenario. This includes integrating with authorised equipment that already exists on a military platform, or running on portable low power electronics carried by a soldier.
- The technology is bi-directional and in-field reconfigurable to meet new or dynamically changing operational requirements. This allows already deployed systems to perform new interoperability and cross-domain functions, and also supports 'over-the-air' changes to be made whenever required.



○ 2.2 The benefit of software ‘adaptors’

- 2iC adaptors within 2iC TRUST allow the rapid integration of systems within each trust domain, by translating their existing protocols (e.g. DDS, Cursor-on-Target, ADS-B, etc) into a common format that can transition from one trust domain to the other, whilst also being in a format that allows content checking to take place, and without the need for further external conversion devices.
- The adaptors enable highly secure yet flexible information exchanges between domains-information such as location, status, images and video from lower trust networks, which might include the integration of a partner force or a COTS device, into a trusted network where the output can be shared.
- This ability enables 2iC TRUST to provide a complete and secure interoperability solution.