



BAE Systems XTS® Cross Domain Access Professional Services

Service Definition Document

1 XTS® Cross Domain Access Professional Services

1.1 Why BAE Systems?

BAE Systems Digital Intelligence supports many worldwide secure government customers safeguard their critical information assets whilst maintaining efficient business operations and mission effectiveness through the provision of high-speed Cross Domain Solutions.

The services and solutions we supply employ Cross Domain products designed in accordance with NCSC design patterns. We work with a variety of third-party vendors to deploy a wide range of Cross Domain Solutions. This includes our own, flagship high assurance Cross Domain Gateway, XTS® Iris, where all security enforcing functions are implemented in hardware using FPGA logic. This hardware-enforced security approach reduces the risk of compromise that is typically associated with lower grade software-based solutions.

BAE Systems proudly boasts the widest portfolio of Cross Domain products available on the market today, from simple one-way diodes to high assurance gateways. Our supply chain and manufacturing facilities are approved by NCSC and we deliver first-class service to our customers. Our heritage, over the last two decades, in protecting the most sensitive networks on the planet, coupled with our industry leading Cross Domain experts makes BAE Systems the world leader in Cross Domain Solutions and the partner of choice for many of the most secure government departments.

1.2 Service Overview

This service concerns Cross Domain professional services including but not limited to, Cross Domain consultancy services, training, integration and deployment services for XTS® Iris Secure Access Gateway (SAG), XTS® CDS Management System (CMS) and third-party Cross Domain products. Procurement of hardware, software and support helpdesk services can be purchased outside of this service offering.

This service is an enabler to establishing a Cross Domain access capability. The capability enables viewing critical data and information, including web browsing, streaming audio and video and remote desktop sessions from remote security domains. The capability removes the need for a swivel chair scenario where users are required to utilise multiple workstations to perform their role, thereby increasing efficiency and reducing infrastructure costs. Users are presented with a window into the differing security domain to enable them to view and interact with remote content securely.

The Cross Domain access capability can be combined with other Cross Domain capabilities such as transfer and voice/video streaming to securely facilitate the movement of files, binary objects and real-time streaming data between highly classified networks (up to TOP SECRET) that would have traditionally been air gapped.

1.3 Service Benefits

Benefits that can be realised as a result of implementing this service and enabling the Cross Domain access capability include:

- Access to world-class Cross Domain experts, reducing upskilling and associated training burden
- Team focus can be maintained on your mission objectives without being distracted by the Cross Domain interoperability challenge

- Cross Domain design, integration and deployment conforming to NCSC architectural patterns
- Reduction in infrastructure costs, enabling one terminal to access multiple security classifications or trust domains
- Enablement of collaboration with external partners without compromising network security
- Enablement of safe access to OT resources from IT business networks without the risk of compromise
- Improvements in efficiency, an increase in operational agility and maintains mission tempo
- Designed and developed in conjunction with UK HMG, reducing accreditation timescales
- Simple, commonly used interfaces and protocols, reducing integration complexities

1.4 Service Features

The features of this service are:

- Integration services for XTS® Iris Secure Access Gateway (SAG)
- Integration services for XTS® CDS Management System (CMS)
- Integration services for third party Cross Domain products
- Test and commissioning of Cross Domain Solutions
- Provision of Cross Domain Solution Architecture services, including but not limited to consultancy/advisory services and production of solution design documentation
- Accreditation support for Cross Domain Solutions
- Training on installation, commissioning and administration of Cross Domain Solutions
- Wider infrastructure provisioning services
- Services provided in line with NCSC's Cross Domain access/browse down architectural patterns

The following additional services are not included as part of this service offering but may be purchased separately via an alternate purchasing mechanism:

- Supply of XTS® Iris Secure Access Gateway (SAG)
- Supply of XTS® CDS Management System (CMS)
- Support services, including service helpdesk and patching provisions

1.5 Example Use Cases

A Cross Domain access capability provides organisations with the ability to reduce infrastructure and increase operational benefits. Below are examples where this capability could help an organisation:

- Securely accessing the Internet from a high-side system providing users with the ability to work on classified and unclassified material from a single workstation
- Remotely managing low-side infrastructure from a high-side system, providing administrators with one view of all networks from a single workstation.

1.6 Ordering and Invoicing Process

The Framework Agreement Call-Off Contract can be utilised to order our services, with invoicing occurring in monthly arrears. Contracts are in accordance with the terms and conditions of this service.

1.7 Related Services

This service can be purchased in conjunction with complementary BAE Systems Digital Intelligence service offerings such as:

- BAE Systems XTS® Cross Domain Transfer Professional Services
- BAE Systems XTS® Cross Domain Voice & Video Professional Services

2 Digital Intelligence: Information Intelligence

We help nations, governments and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulation and transform their operations.

Our exclusive accreditations are testament to the quality of work we provide: We're one of only a handful of companies certified by GCHQ (UK Government Communications Headquarters) and CPNI (Centre for the Protection of National Infrastructure) as quality-assured cyber incident response providers and are the first company to receive accreditation for both threat intelligence and penetration testing on the Bank of England's CBEST scheme.

Enabling our customers

We use these same tools and skills to analyse big data for companies to provide them with solutions that enable them to tailor customer interactions and build trust. For example, we build targeted, interactive websites, we analyse what infrastructure companies need and then future proof it for them, and our data accuracy is so good that we can help pinpoint sources of infectious diseases and ensure treatments are delivered quickly and efficiently. We also create efficiencies and performance for Governments and businesses through delivering integrated collaboration models to align behaviours to the customers' interest.

Solutions you can trust

So, whether it's protecting nations and businesses from cyber threats, helping police and national security to identify and bring down terrorists, or analysing big data to ensure businesses prosper our technology, processes and people are set up to deliver the best results.

What do we provide?

- We offer a broad portfolio of on premise, managed and cloud-based products and services that are battle proven against the world's most dangerous threats.
- As the leading provider of threat intelligence to the US and UK governments, we provide business defence no one else can match
- And it's not just cybercrime we defend against. We also help companies and Governments defend against increasing regulatory burdens and communication infrastructure changes
- Intelligence is at the core of what we do:
 - o Cyber defence: Monitoring, analytics, email and cloud-based security, investigation and incident response solutions
 - o Financial Crime Prevention: Identifying, combating and preventing financial threats, risk, loss or penalties
 - o Communications Intelligence: Next generation intelligence and cybersecurity solutions for national security and law enforcement; compliance solutions for CSPs
 - o Digital Transformation: Using data to pursue new business models, enhance customer engagement and improve business operations

