QUANTUM FIREWALL

The Era of Cross Domain Innovation

Connecting forces, intelligence, police and government in multidomain

August 2024

arbit

Lets Connect Forces

Arbit Cyber Defence Systems, based in Copenhagen, Denmark, was founded by Rasmus Borch and has for almost two decades provided Cross Domain Solutions based on quantum technology tailored for organizations with stringent security and confidentiality requirements, such as intelligence agencies, police, defence, and infrastructure.

Our domain: Arbit legacy and deep domain knowledge originates from the intelligence community, focusing solely on Cross Domain Solutions designed to securely manage data transfers between networks of different security classifications and guarantee a unidirectional communication channel that enhances security while reducing costs, human error, and insider threats.

Arbit solutions are proven in Bold Quest from Georgia, US to Finland and are RUGGED ready to be deployed in challenging conditions on the battlefield, offering a Gateway (IEG) with reliable data management and C2 communication between security domains in military operations.

Certification: The company's most notable certification is the German Evaluation Assurance Level (EAL7+) for its Arbit Data Diode, a rare and high-level accreditation, NATO COSMIC TOP SECRET, which signifies the product's compliance with the most rigorous security standards for information technology products.

Clients: Arbit's expertise has attracted clients from all of Europe, the Middle East and Asia. Including the Danish Ministry of Defence Acquisition and Logistics Organisation (DALO) who has entered into a 20-year framework agreement with Arbit. This partnership is aimed at providing the Danish Armed Forces with advanced cross-domain solutions, underscoring a long-standing relationship between DALO and Arbit to enhance digital security and operational effectiveness.

Contribution: In recognition of our contributions to cybersecurity, Arbit became the first company in Europe to receive the "Cybersecurity Made in Europe" label from the European Cyber Security Organization (ECSO).

And with our participation in international defence forums and projects, such as NATO EDGE, NATO CWIX, Timber Express, and European Defence Fund (SESIOP) we hope to demonstrate our commitment to advancing cybersecurity solutions that meet the needs of protecting and securing Governments or organizations around the world.

It's all about Trust: Arbit's success is shared through collaboration with clients, selected technological and strategic partners. Because for the founder, it is all about Trust. Let's Connect Forces.

Content

Lets Connect Forces 2

Arbit in Goverment, Comcenters and Serverrooms 4

Partners and membership 5

For Armed Forces 11

From PINK to GREEN at NATO CWIX 24 18

In the Navy 19

Advanced Cross Domain use cases 20

Interchangeable modular hardware platforms 22

New in critical infrastructure: Asian waterplants 24

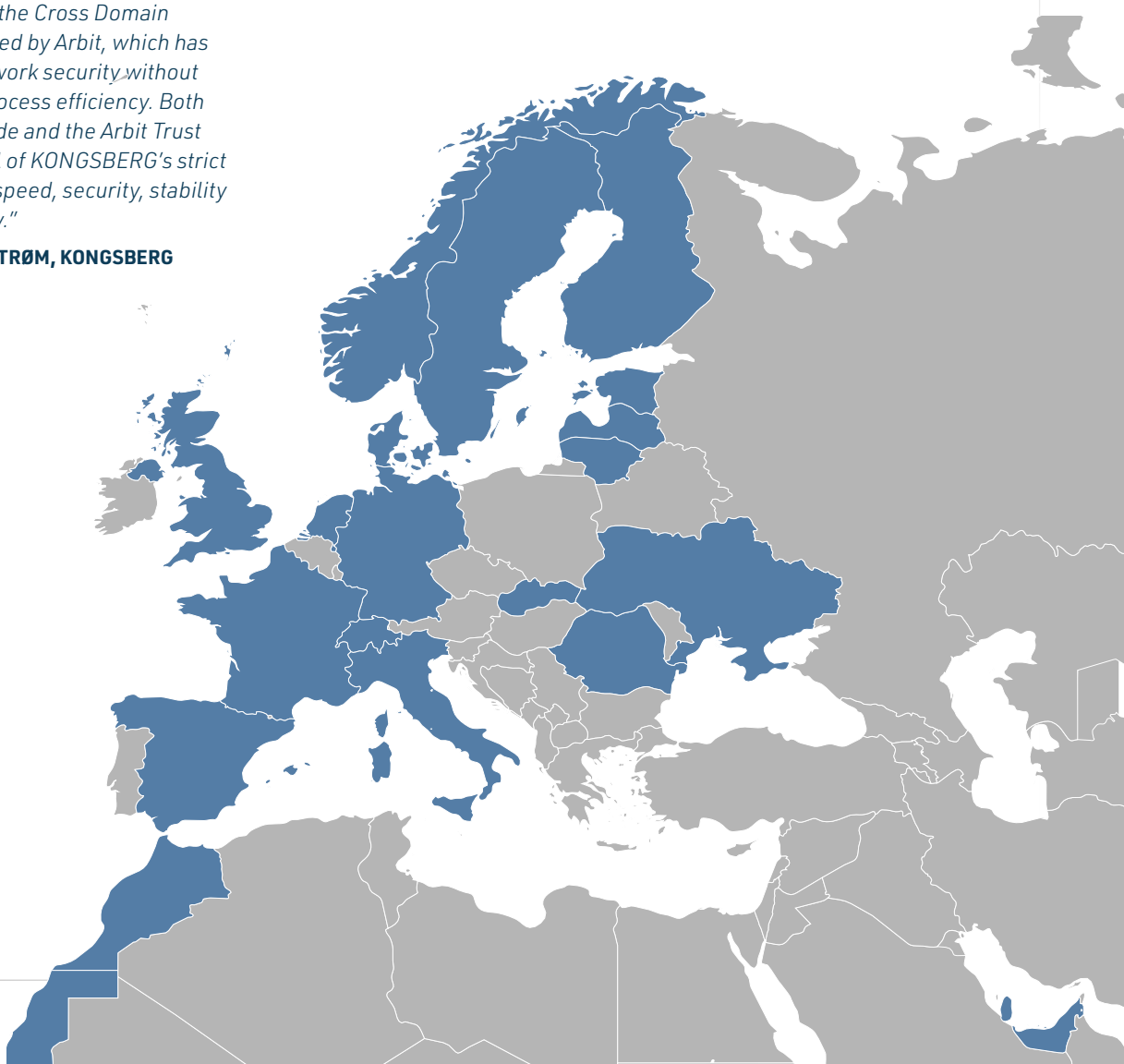
Enodia Bridge by Allsafe.house 25

Galvanic Seperation, Krypto, Tempest and anti-malware 26

Arbit supports 27

"KONGSBERG DEFENCE & AEROSPACE has implemented the Cross Domain Solutions developed by Arbit, which has improved our network security without impairing work process efficiency. Both the Arbit Data Diode and the Arbit Trust Gateway meets all of KONGSBERG's strict requirements for speed, security, stability and manageability."

– CIO, JAN HELGE STRØM, KONGSBERG



Arbit in Goverment, Comcenters and Serverrooms

Together with Statens IT, Arbit has tailored a solution based on the Arbit Data Diode Hardware technology providing hard segmentation and boundary protection for ministries, along with advanced anti-malware platforms in a redundant and resilient architecture.

Friends and partners

ESTONIA

USA

FINLAND

NETHERLAND

SWEDEN

USA

GERMANY

SWEDEN

Member of

DENMARK

DENMARK

DENMARK

DENMARK

Reference customers

DANISH MINISTRY OF DEFENCE ACQUISITION AND LOGISTICS ORGANISATION
WWW.FMI.DK/ENG

KONGSBERG
WWW.KONGSBERG.COM

THE AGENCY FOR GOVERNMENTAL IT SERVICES
WWW.STATENS-IT.DK/ENGLISH

TERMA
WWW.TERMA.COM

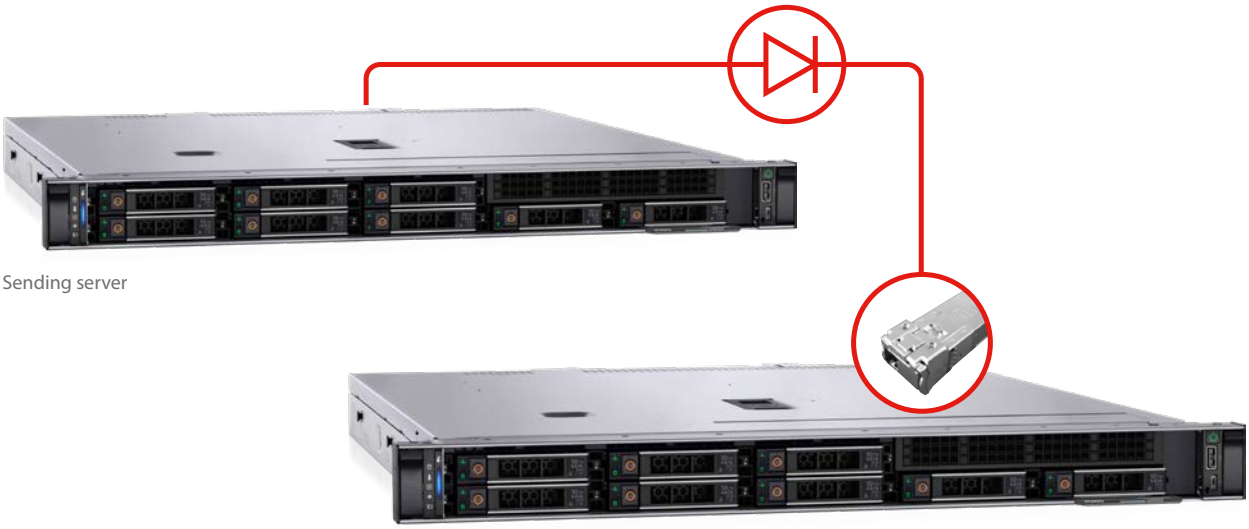
DATADIODE

Quantum Firewall – Semiconductor

When protecting data confidentiality in a classified network, resources are spent to ensure air-gap separation between multiple classified domains. This usually includes filtered power supplies, galvanic separation, shielding/TEMPESTing, and more.

After investing several resources, it is essential that the selected cross-domain solution does not break this fundamental concept.

The Arbit Data Diode is a physical data diode based on optics and semiconductors. The diode's security feature is enforced at the quantum level, hence the predicate Quantum Firewall. There is no software, microcode, or other processor logic involved. The diode principle is proven in physics, allowing it to receive the world's highest security certification: Common Criteria EAL7+ by BSI, Germany.



Contrary to software solutions that ensure only the logical separation of networks, optical data diodes enforce physical separation of networks without any return channel due to the highest evaluation and certification in the world (EAL7+). The Arbit Data Diode 10 GbE fulfills advanced needs for stability, scalability, throughput and low latency, together with a competitive total cost of ownership. The best official client case is 24 files per. sec. nonstop for 14 days without any data loss.

Fast, hardware-based network security

Unilateral data transfer between networks without the risk of unauthorized remote access.

Most two-way communication can be compromised, and even the most well-protected networks can be penetrated.

The fail-safe solution is to physically separate high security networks from low security networks. While this is the most secure solution, it also severely reduces productivity as it prevents data from being transferred directly between the networks.

However, with the data diode technology you can allow one-way data transfer without compromising the confidentiality and integrity of the air-gapped network. Using a single fiber-optic connection with the EAL7+ certified module, the data diode ensures one way data transfer between separated networks of the same or different classification.

While data is only allowed to pass in one direction, it can never be transmitted the opposite way. This means that no intruders can use the connection to remotely access or steal data from your critical network.

Software vs. hardware solution

	FIREWALL	SOFTWARE DATA DIODE	ARBIT DATA DIODE
100% protection against data theft	No	No	Yes
100% protection against hackers	No	No	Yes
Secure one-way connection	No	No	Yes
Protected by laws of physics	No	No	Yes

Interchangeable modular hardware – All our software runs on all our hardware platforms.
For more details on this, see our advanced use cases (pages 17-18).

The Arbit Data Diode is a physical data diode that establishes a secure one-way connection. The transmission is handled by two dedicated servers.

The Arbit Data Diode offers a physical seamless one way data connection, maintaining full galvanic network separation (no covert channel possible). Therefore, the Arbit Data Diode is even safer than manual data transfer, yet offers the same convenience as a normal network connection.

The Arbit Data Diode has achieved the Common Criteria EAL 7+ certification and meets the ISO-15408 requirements. The Arbit Data Diode is accredited NATO COSMIC TOP SECRET, EU TOP SECRET and YDERST HEMMELIGT by CFCS, DK

CC EAL7+ By BSI Germany · ACCREDITED NATO COSMIC TOP SECRET AND EU TOP SECRET · Fiber and Copper Connectors

Datadiode EAL 7+

Identical interfaces on the sending side (Pitcher) and receiving side (Catcher) of the data diode

BENEFITS

- 100% secure hardware data diode
- Full galvanic separation
- High throughput and transfer rate
- High stability and low TCO and maintenance
- Proven track record for 15 years
- User-friendly web interface
- Powerful add-ons to control content moving through the data diode
- Full integration with OPSWAT advanced anti-malware platform
- Easy and secure configuration management
- Combine with TEMPEST level-A

FEATURES

- 1 GbE or 10 GbE versions (both Common Criteria EAL7+ certified)
- Accredited NATO COSMIC TOP SECRET and EU TOP SECRET
- No maximum file size (only limited by disk space on proxy servers)
- 64 data channels per diode
- Data channel priority (on transaction basis)
- Supports up to 24 streaming channels (logging, video, radio via UDP)
- High availability with peer-to-peer recovery
- Syslog and notifications by email
- Software runs on hardened Linux

SUPPORTED PROTOCOLS

- Mail (SMTP)
- Simple File Transfer (FTP, SFTP)
- Windows share forwarding (SMB)
- Windows share mirroring (SMB)
- Network File System share forwarding (NFS)
- Network File System share mirroring (NFS)
- Time synchronization (NTP)
- Streaming UDP, TCP via UDP
- REST API Forwarder (HTTP, HTTPS)
- OPSWAT Integrations

KEEP YOUR SYSTEMS SECURELY UPDATED

- WSUS
- Linux repository
- Anti Virus updates

TEST

DESCRIPTION	GIGABIT
Throughput	700 Mbps
Transactions per second	18,0 (512 KB files)
Transaction failure rate	0 (out of 5 mio files)

CC EAL7+ By BSI Germany | ACCREDITED NATO COSMIC TOP SECRET AND EU TOP SECRET | Fiber and Copper Connectors

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

GATEWAY

Data release from secure networks

Safe release of approved data from highly secure or air-gapped networks

Moving data into a secure network is easily handled by a data diode. However, when data is required to leave a secure network, this is often accomplished using USB-sticks or other portable devices, along with all the inherent security risks.

The Arbit TRUST Gateway (ATG) eliminates the need for manual data transfer and ensures that only approved data is allowed to leave the secure network, making this critical operation as safe as possible. The ATG platform also supports browse down and remote desktop access set up from high to low.

The ATG uses signing technology to identify the source of the released data. Only approved source systems and authorized individuals can sign data, which is then allowed to pass through the gateway. By adding ATIR - the Arbit Trusted Information Release portal, a number of organizational security requirements can be added such as two factor release.

The ATG is based on Common Criteria EAL7+ certified Arbit Data Diode technology. This protects against attacks from the receiving side as well as the transmitting side. In addition, the system is based on hardened Linux.

The ATG can perform several content checks/filtering, including checks/filters developed by Arbit as well as third party checks/ filters like multi scanning products using our Open API.

The Arbit TRUST Gateway (ATG) ensures that data released from a protected network is both source and content checked according to company security policy, so that no rogue process or system can send data through or even piggyback information on approved transactions.

The ATG acts like a secure platform where several COTS or custom checks can be performed. The ATG is based on the robust Arbit Data Diode technology and consists of two Arbit Data Diodes that are connected in serial.

This creates an isolated VOID network which is not accessible from neither the high side nor the low side. Therefore, the isolated VOID is the perfect area for final filtering and checks as it cannot be manipulated.

All configuration and program code are stored on read only media, so its impossible for an attacker to change the system in any way. Rebooting the system is guaranteed to restore the approved configuration and the Arbit program code.

Certified CC EAL 7+ | Accredited NATO SECRET and EU SECRET | Built on Data Diode technology | Content Verification

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

GATEWAY

Benefits, features and integrations for Arbit Gateway

BENEFITS

- Replaces non-secure manual data transfer
- Proven transmission stability using Arbit Data Diode technology
- Integrates with existing company infrastructure Open API for building custom content verifiers (C++ and Java)
- Supports 'Releasing and Drafting Officer' function using the Arbit Trusted Information Release portal
- Full integration with OPSWAT advanced anti-malware platform
- Optional external content verifiers and AD-look up verifying sender or content

FEATURES

- Built on Data Diode technology
- Based on 1U rack-mountable units
- All zones with galvanic separation
- Fiber or copper connectors to external networks
- Read-only boot device
- Low power consumption
- Low latency
- Accredited NATO SECRET and EU SECRET

INTEGRATES WITH

- SYSTEMATIC SitaWare (Command and control software)
- Arbit Trusted Information Release Portal (Two factor release of data)
- Arbit Desk Top Gateway (Browse down)
- Arbit WEB Gateway (Web access)

COMPARE WITH OTHER METHODS FOR DATA EXPORT	USB	CD-ROM	Arbit Trust Gateway
Avoids two-way connection when releasing data	NO	YES	YES
Verifies source of released data	NO	NO	YES
Verifies data content according to security policy	NO	NO	YES
Ensures release work-flow policy is upheld 24x7	NO	NO	YES
Low latency in release of data	NO	NO	YES
Automatic threat & content scanning using OPSWAT MetaDefender™	NO	NO	YES

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

For Armed Forces

RUGGED to Connect Forces
RUGGED Data Diode
RUGGED IEG Gateway

Picture by the courtesy of General Dynamic.

Arbit Cyber Defence has a 20-year agreement with The Danish Ministry of Defence Acquisition and Logistics Organisation (DALO), focusing on digital cross-domain solutions for the Danish Defence.

This long-term framework is to increase network security across various military units, from HQ server rooms to frontline units.

RUGGED DATADIODE

Tested to operate in the battlefield

Tested in Bold Quest from the heat of Savannah and to the cold in Finland

Unilateral data transfer between high security networks without the risk of unauthorized remote access or data stealing

Even the most secure connections can be compromised, and even the most well-protected networks can be penetrated. The fail-safe solution is to physically separate high security networks from low security networks. While this is the most secure solution, it also severely hampers productivity since it prevents data from being transferred between the networks.
However, with the Arbit Data Diode you can allow one-way data transfer without compromising the integrity of the air-gapped network. By using a single fiber-optic connection that can only send light in one direction, the Arbit Data Diode transports data from less-secure networks, such as the open Internet, to secure networks.
While data is allowed to pass one way, it can never be transmitted the opposite way. This means that no intruders can use the connection to remotely access or steal data from your critical network.

- Common Criteria EAL7+ Certified Hardware
- Accredited NATO COSMIC TOP SECRET and EU TOP SECRET
- The Arbit Data Diode is a 100% secure physical data diode
- Proven software stability through 15 years of service
- User-friendly web interface
- Integrates with Microsoft server solutions
- Quick installation and configuration
- Powerful add-ons to control content moving through the diode
- Full integration with OPSWAT multi anti-malware-scanning and CDR
- 700 Mbps throughput

MILDEF

Ruggedized by MilDef

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

RUGGED DATADIODE

FEATURES

- Maximum file size limited only by available disk space
- 64 data channels per diode
- Data channel priority (on transaction basis)
- Supports up to 24 streaming channels (video, radio, etc.)
- Back Pressure in case of critical diskspace
- Notifications by email, syslog, and SNMP
- User-friendly web-interface
- No daily maintenance
- Software runs on hardened Linux
- Filters for SitaWare Secure Gateway (SSG)

TECHNICAL DESCRIPTION

The Arbit Data Diode is a physical data diode that establishes a physically secure one-way connection with a single fiber-optic cable. The transmission is handled by two dedicated servers.

The sending server is called a pitcher, and the receiving server is called a catcher. No data can be transported from the receiving network to the transmitting network. Therefore, the Arbit Data Diode is just as safe as manual data transfer yet offers the same convenience as a normal network connection.

The Arbit Data Diode has received the Common Criteria EAL 7+ certification, accredited NATO COSMIC TOP SECRET and EU TOP SECRET, listed on NATO IAPC, and meets the ISO-15408.

SOFTWARE VS. HARDWARE SOLUTION

	FIREWALL	SOFTWARE DATA DIODE	ARBIT DATA DIODE
100% protection against data theft	No	No	Yes
100% protection against hackers	No	No	Yes
Secure one-way connection	No	No	Yes
Protected by laws of physics	No	No	Yes

SUPPORTED PROTOCOLS

- Mail (SMTP)
- Simple File Transfer (FTP, SFTP)
- Windows share forwarding (SMB)
- Windows share mirroring (SMB)
- Network File System share forwarding (NFS)
- Network File System share mirroring (NFS)
- Time synchronization (NTP)
- Streaming UDP, TCP via UDP
- REST API Forwarder (HTTP, HTTPS)

WORKING CLIMATE / TESTED ENVIRONMENTS

- Temperature shock
- Salt/fog
- Vibration
- EMC/EMI Environment

SIZE

- Based on 1U, 19"/2 components
- Data diode 1U 2x19"/2 units

POWER

- Data Diode will run on 12-24V
- Diode < 170W

SECURITY CERTIFICATION

- The Target of Evaluation (TOE) ensures NO backflow is possible.
- Accredited NATO COSMIC TOP SECRET and EU TOP SECRET by CFCS, DK.

Picture by the courtesy of General Dynamics

RUGGED GATEWAY

Information Exchange Gateway (IEG) in multi-domain operations

C4ISTAR
– Securely exchange C2 military information.

The Arbit EAL7+ Certified C4ISTAR gateway allows you to securely exchange C2 information between coalition forces on the battlefield, supporting both automated and manual release as well as import of data.

SECURE AND TIMELY DATA EXCHANGE

Smaller or larger military formations that have deployed Cross Domain solutions to obtain the highest security, still have the essential need to exchange timely C2 information between subordinate units and/or coalition forces. The Arbit C4ISTAR gateway supports safe and fast data exchange, supporting both automated and manual release and import of data. The Gateway is accredited NATO SECRET and EU SECRET.

Since the import and export of data are subject to many security procedures and regulations, the Gateway supports a full set of security procedures that can be required for data exchanges.
Typically, classifications, markings, release ability, formats, and origin of data must always be verified and checked before data can be released or exchanged. In addition, some types of information exchanges are extremely time sensitive, such as blue force tracking and Cross Domain calls for fire. The Arbit C4ISTAR gateway allows you to set validations and checks to meet your security profile, including release procedures (two-factor release), data content validation, validation of signing, classification, and other filters such as multiple virus scanning.

Arbit C4ISTAR Gateway is built on Arbit's hardware-based Data Diode technology and therefore offers a continued network separation with no backflow possible.

The Arbit C4ISTAR gateway can be delivered in two variants – a server room version and a rugged version (only hardware is different). The rugged C4ISTAR gateway is designed and built to operate on the battlefield under the most challenging conditions. All units are 1U 19"/2 and a full gateway is only 3U (UPS and power supply excluded) equipped with NATO standard connectors and designed for vehicle mount.

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

RUGGED GATEWAY

FEATURES

The Arbit EAL7+ Certified C4ISTAR Gateway platform allows implementation of different security profiles and offers a range of filters and add-ons. The most important feature is that the robust and open API of the Gateway allows you to program and build your own national security profile independent from any contractor support. This is the highest level of security you can get - you own the data as well as the processes.

Integrates with

- SYSTEMATIC SitaWare (Command and control software)
- Arbit Trusted Information Release platform (Two factor release of data)
- Arbit Desk Top Gateway (Browse down)
- Arbit WEB Gateway (WEB access)
- Filters for SitaWare Secure Gateway (SSG)

Working climate / tested environments

- Temperature shock
- Salt/fog
- Vibration
- EMC/EMI Environment

Logging

Provides full audit log and syslog

API

Offers open API for building custom content filters (C++ and Java).

Malware Protection

As an OPSWAT partner, the C4ISTAR Gateway integrates with OPSWAT MetaDefender multi anti-malware scanning and CDR.

Verification of Data Signatures

Uses signing technology to securely identify the source of released data. Only approved source systems or individuals can sign data which is then allowed to pass through the gateway.

Two-factor Authentication

Supports signing as standard and NATO Clearing house functions such as Releasing and Clearing officer.

Size

- Based on 1U, 19"/2 components
- Data diode 1U 2x19"/2 units
- Server 1U 1x19"/2
- Full gateway 3U 19"

Power

- Both Gateway and Data Diode will run on 12-24V
- Server < 200W
- Diode < 170W
- Full Gateway less than 800W

Security certification

- The Target of Evaluation (TOE) ensures NO backflow is possible.
- Accredited NATO SECRET and EU SECRET by CFCS, DK

Cross Domain for Piranha V

Arbit TEAM is part of the Danish sub-suppliers to the Piranha V, from General Dynamics, to the Danish Army.

Data Centric security and Cross Domain solutions for multidomain operations

Cross Domain Solutions and Data Centric security for multidomain operations

Building a multi-Domain Operations network naturally includes discussions of Data Centric Security and information exchange between different security domains. Cross-Domain Security and Cross-Domain Solutions (CDS), such as gateways, are essential components of NATO's data-centric security framework.

- Cross-Domain Solutions (CDS) like data diodes and gateways or IEGs, are specialized security systems that control and monitor the transfer of information between different networks and security domains to prevent data leaks and ensure that only appropriately sanitized and approved data crosses domain boundaries.
- Data Centric security (DCS) protects the representation of information directly and ensures that data retains its integrity and confidentiality when moving across domains and that only users with the precisely correct user rights can access (and decrypt) specific data within that network and security domain.

The challenge designing DCS

Data-centric security is designed to address the evolving threats in cyberspace, ensuring the integrity, confidentiality, and availability of mission-critical data across its operations and among its member nations.
The challenge with the Data Centric security approach, from a classification security perspective, however, is that the specific network that stores a HIGHLY CLASSIFIED file, automatically gets the same HIGH classification if that data is available unencrypted – even for a short while.
This means that if a user accesses and opens a file (and thereby decrypts it) that is NATIONAL TOP SECRET on a network, the network will automatically become NATIONAL TOP SECRET with all compliances, regulations, rules concerning interconnections, information sharing across nations, etc.

So, if a piece of classified data is sufficiently encrypted, the encrypted data is no longer classified and could be stored or transmitted on networks with a lower classification. However, as soon as the data is unencrypted (even in memory on a user's computer), the network connected to the computer must have the appropriate classification level. E.g. secret information cannot be decrypted on the internet.

Type 1: Classical border protection – both classified and unclassified data are accessible inside the network

Type 2: Classical border protection AND Data Centric Security – Classified data inside the network is stored encrypted

Type 3: Classical border protection AND Data Centric Security – EXPORTED classified data is not accessible

CDS and DCS are combined forces

No doubt that Data Centric security will be a huge step forward in ensuring the right access to data stored within a network compared to how it has been implemented in many places until now.

Yet Cross Domain remains needed for bridging information transfer between networks of different classifications, and Cross-domain solutions are a critical link in the security chain, enabling safe, controlled, and efficient sharing of information across different security environments while upholding the principles of data-centric security.

Also, in the future exchange of C2 information in multidomain operations.

From the intelligence community, NATO personnel, and other professionals in CWIX, it's a common understanding that DCS will not replace existing security measures for confidentiality, integrity, and availability, including boundary and network segmentation. This resonates with the NATO Multi-Domain Operations Conference in Copenhagen, where the need for Cross Domain, with C2 information, was discussed as there is an urgent need to exchange information between NATO networks, NATO nations, and non-NATO entities.

From PINK to GREEN at NATO CWIX24

A succesfull test and proof of interoperability

Encouraged by NCI, several clients and partners of Arbit participated in the Coalition Warrior Interoperability Exercise (CWIX24) in Bydgoszcz, Poland. Arbit successfully connected PINK (HIGH) to GREEN (LOW). Arbit released and validated NATO labeling through our Gateway hardware. With the test providing promising and successful results, it showed our domain expertise. The Gateway solution effectively supported (C2) information exchange from PINK to GREEN, fully complying with NATO STANAG 4774 and 4778. With successful connections between forces and hosted visits from Danish, Finnish, German, Italian Defence and other allies, it shows the importance of international collaborations.

Arbit is fortunate to be a part of CWIX24 and to be supported by the experience of the national lead and Commander Karsten Horn, Branch Chief of Interoperability at the Cyber Division at Danish Defence Acquisition and Logistics Organisation (DALO). Arbit's success in CWIX24 therefore showed our commitment to advanced interoperability goals.

In the Navy

With a minimal footprint, the Arbit Data Diode protects information and systems on Naval Vessels.

Arbit is deployed within several Naval Installations and ensures that critical information doesn't fall into the wrong hands, and systems are not destroyed by cyber-attacks.

A use case involves requirements for unidirectional UDP communication between different security domains on a Naval vessel, demanding a Cross-Domain Solution that can perform in harsh environments and adhere to the highest security standards, all with a minimal physical footprint. In this case, the Arbit Data Diode fulfills all three requirements: ruggedized for military use, certified, accredited, and without taking up any rackspace.

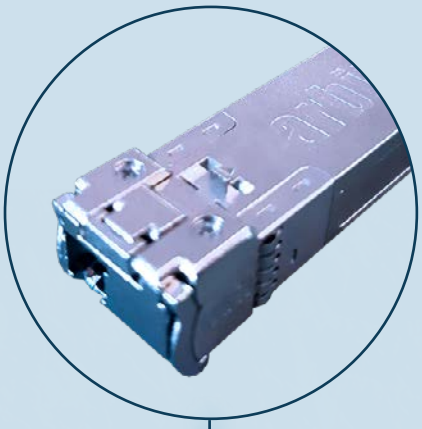


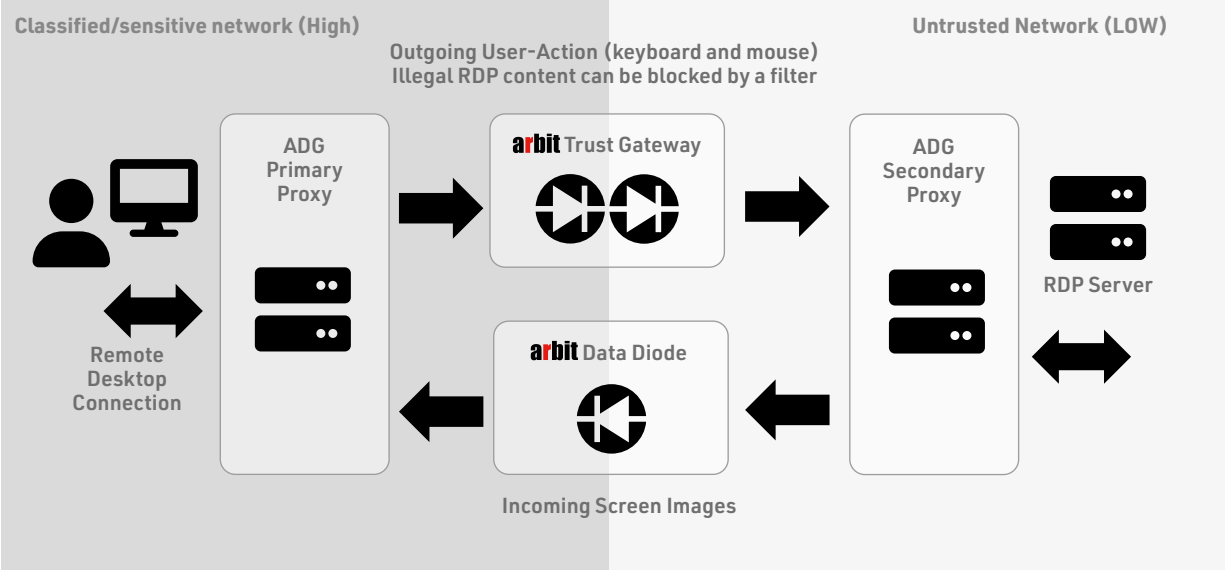
Foto: Danish Patrol Vessel Ejner Mikkelsen, captured in the arctic by Captain Troels Sundwall.

Advanced Cross Domain use cases

With Data Diode and Gateway for Armed Forces, Intel, Police and Government, eliminating unauthorized remote access.

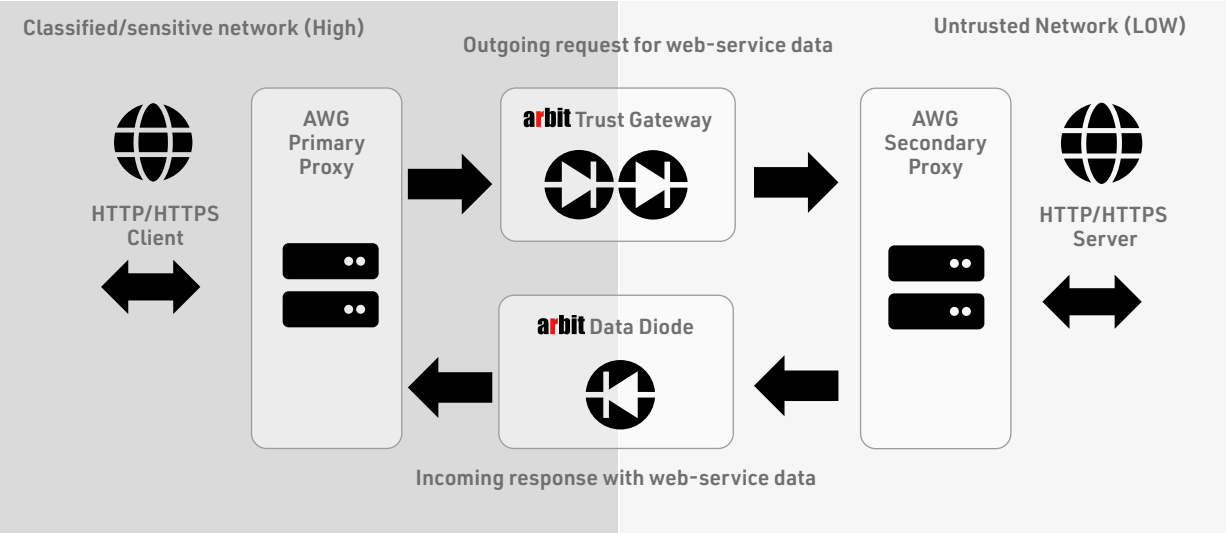
ADG – Simplify Remote Work with Secure Desktop Access

When a user regularly works across multiple networks, the Arbit Desktop Gateway (ADG) allows remote desktop access via RDP (Remote Desktop Protocol) from a higher classified network to a lower classified network. One Arbit Trust Gateway handles mouse and keyboard activities, while another manages screen image imports through either an Arbit Data Diode or Arbit Trust Gateway. This setup removes the necessity of connecting all networks directly to each user's workstation, simplifying the hardware setup. Bi-directional is obtained via two separate unidirectional channels.



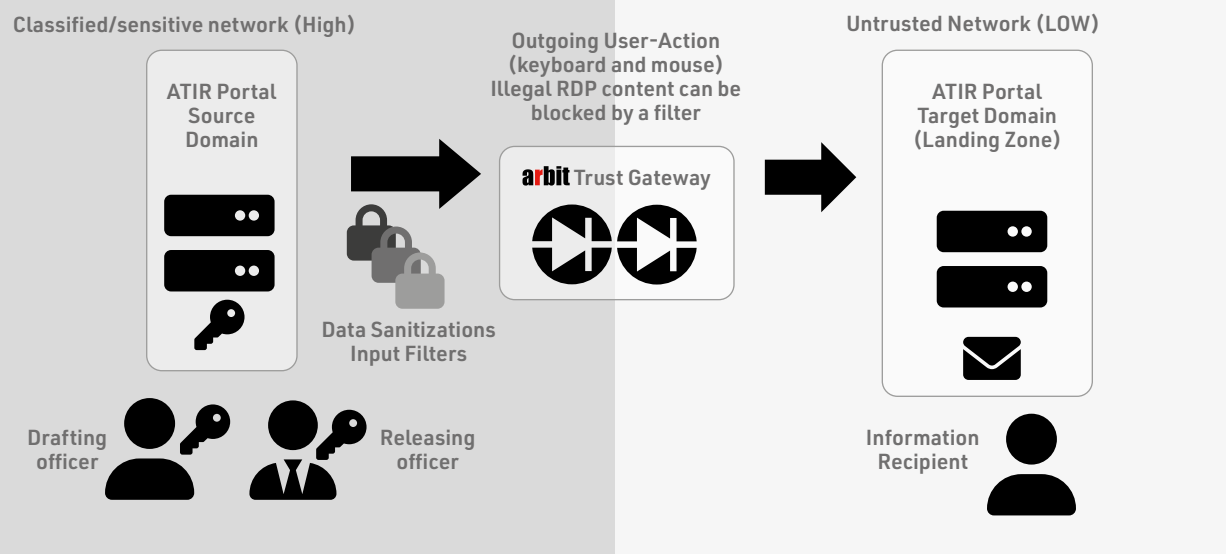
AWG – Boost Productivity with seamless web secure services across military and civilian domains

Together with the Arbit Trust Gateway, the Arbit Web Gateway (AWG), allows you to build controlled and seamless dataflows using the ubiquitous http(s) protocol. It's a convenient, secure, and efficient way to integrate cross-domain capabilities into your existing systems. It is the trusted way to exchange data seamlessly between different security domains. Bi-directional is obtained via two separate unidirectional channels. The Gateway is also known as IEG.



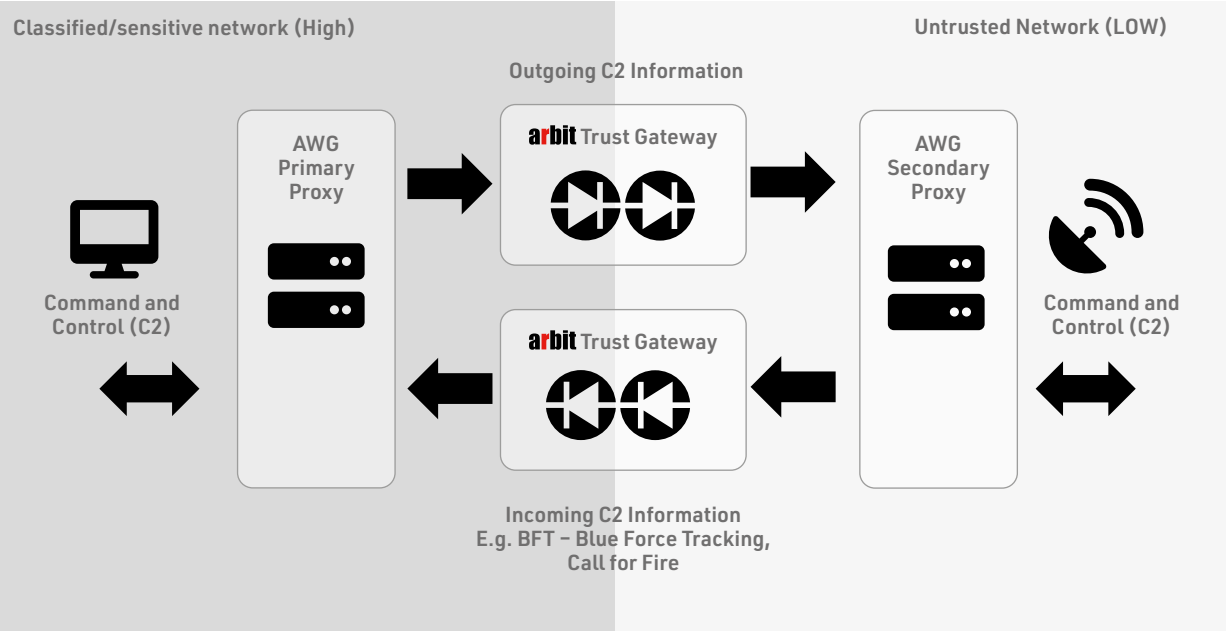
ATIR – Approved and Controlled data release Cross Domain

The Arbit Trusted Information Release (ATIR) is a portal that allows controlled sharing of unstructured information, like documents, from a higher classification domain to a lower one. The release must be performed by two individuals: the drafting officer prepares the release, and the releasing officer approves it. Bi-directional is obtained via two separate unidirectional channels.



CDS – Enhance Operational Efficiency with Seamless Data

Import/Export Cross Domain The Arbit Cross Domain Solution (CDS) is a platform for controlled and seamless data transfer across multiple security domains. It functions with two Arbit Trust Gateways (ATG), one for data import and one for data export, all the while maintaining galvanic separation. Bi-directional is obtained via two separate unidirectional channels. CDS can be used in server rooms or RUGGEDIZED to withstand even the harshest of environments.



Interchangeable modular hardware platforms (Units)

Units consist of servers with read-only boot media and configuration stored on smartcards. They are used for: Arbit Trust Gateway, Arbit Data Diodes with virtual proxy servers

Dell XR11 | Network connectors: Always add transceivers as per requirement

Dell XR11 – High performance | Network connectors: Always add transceivers as per requirement

ARBIT COTS Unit | Network connectors: Always add transceivers as per requirement

MILDEF RUGGEDIZED | Network connectors: 1x1GbE fiber multimode

Interchangeable modular hardware:
All our software runs on all our hardware platforms.

Interchangeable modular hardware platforms (Devices)

Devices consist of servers with writable disks and are configured via a web-based GUI. They are used for: Arbit Data Diodes (no need for virtual proxy servers)

DELL R350 | Network connectors: 2x1GbE copper + add transceivers as per requirement

Arbit Core Kit | Network connectors: 1xSFP+ (only compatible hardware, i.g. BroadCom)

Arbit Cots Device | Network connectors: 2x10GbE/2x1GbE copper + 2x 10GbE fiber single mode

NEW

Now in Critical infrastructure
Asian waterplants

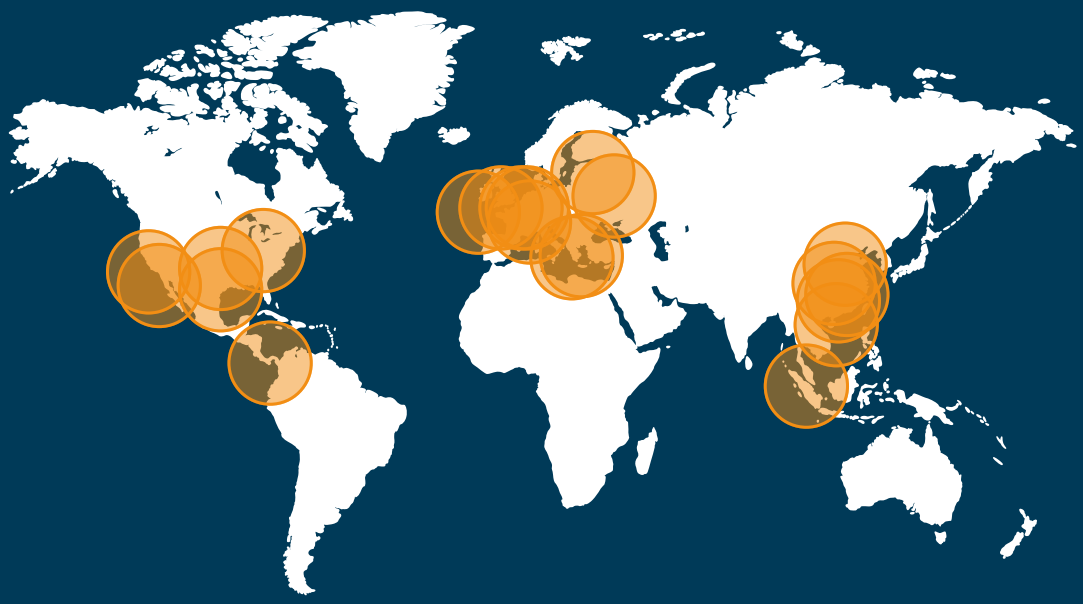
Free 30 days scoring of your traffic on our collector in the cloud. You can see how much we would filter on your specific traffic. Requires that your NAT firewall can send Meta Data to our destination. I.e. syslog.

(Also possible to identify traffic leaving your networks towards our IOCs)

Enodia Bridge

- **Additional hardening of your public facing networks with dynamic Block lists on the L2/L3 layer.**
- **Additional DNS protection with dynamic Allow and Block lists.**
- **Encrypted DNS (DoH, DoT & DoQ).**
- **Optional DNSSEC end-to-end.**

- Around 1 million lines in our signature IP Block List. Updated every 10th minute.
- More than 10 million FQDNs in our DNS firewall. Updated every hour.
- Harvesting IOCs from our own honeypots in Europe.
- Can run on your own hardware.

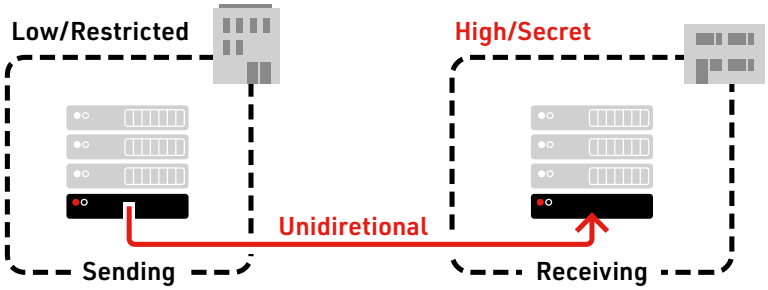


Supplied by Arbit

allsafe.house

Galvanic Separation in Cross Domain High Security Networks

Our solution's architecture ensures galvanic separation of hardware of different classification levels. It adheres to clearance distances, so that no microprocessor operates with more than one network CLASSIFICATION. This design also enables our hardware to meet TEMPEST standards, as only one network CLASSIFICATION exists inside each physical box.



Sending and Receiving units can be separated into a single rack, different racks,or different locations. Connected only with a single fiber.

secunet – protecting digital infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data (up to EU and NATO SECRET), applications and digital identities. secunet specialises in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed at the German Stock Exchange and generated revenues of 393,7 million euros in 2023.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security

EUROTEMPEST

Eurotempest develops high-assurance IT products and systems for defence- and government use. Their products are used by national- as well as central authorities, throughout EU and NATO in more than 20 countries.

Eurotempest customers can select TEMPEST versions the latest IT products technology with confidence that formal requirements and standards are met.

Mix Tempest level-A protection with EAL7+ cyber security in one device to protect and manage CLASSIFIED DATA

Eurotempest employees have years of experience from various high-assurance projects involving TEMPEST, crypto and secure systems development. They work directly with most of the major manufacturers of IT equipment and are technology partners to companies like Panasonic, HP, DELL, Fujitsu, NEC/Sharp and Allied Telesis.

OPSWAT. – Perimeter protection Cross Domain, on the HIGH side

OPSWAT's motto is "Trust no File. Trust no Device." The Arbit/OPSWAT partnership excels at managing the challenges of impex 'Ing files between one domain to another. Addressing malware and viruses is complex and should be handled at the network perimeter to avoid over-reliance on endpoint protection. OPSWAT uses the world's leading multi-scanning technology, with up to 33 anti-malware engines, to detect and remove up to 99.6% of the world's top 10,000 threats. OPSWAT's Content Disarm and Reconstruction (CDR) technology, disarms and de-weaponizes over 180 file types, stopping zero-day threats. For files that can't be processed by CDR, OPSWAT's emulation-based sandbox performs a final check at near wire-speed, ensuring files are clean before import.

Arbit supports

TEAM RYNKEBY

SIF

POLITI FORBUNDET

DIM

Idrætsforeningen Flyvestation Karup
- medlem af Dansk Militært Idrætsforbund

240169 · 2024-08

Want to know more about our solutions?

Scan the QR-code to download all our product information.

arbit

Immerkaer 54 | 2650 Hvidovre | Denmark | Email: info@arbitcds.com | VAT DK38991469 | www.arbitcds.com