Cross Domain Hybrid Application Framework

Secure by Design : A reusable pattern for seamless interoperability & cross domain collaboration
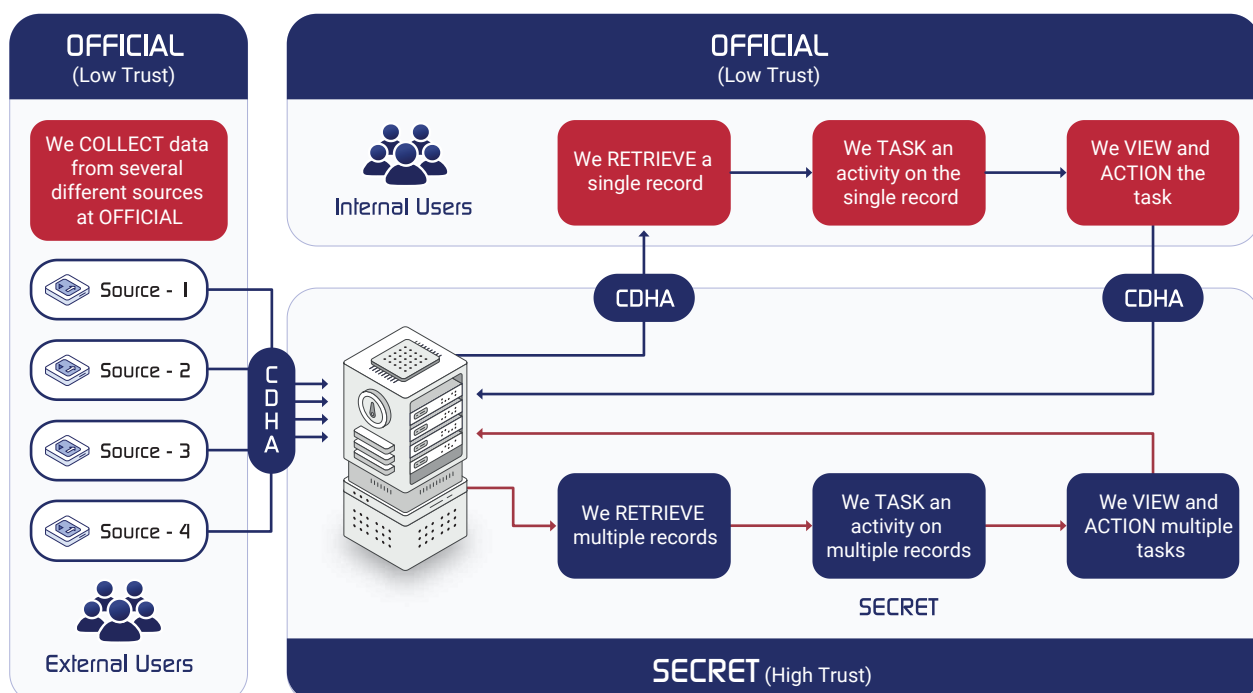
acubed.it
Designing Secure Applications

The Problem

Cross domain working is one of the National Cyber Security Centre's (NCSC's) key problem areas

Acubed.IT has identified numerous use cases across HMG where data is collected from several sources at OFFICIAL. When this data is aggregated, it's overall content can provide valuable information to Hostile State Actors. It is therefore then classified at SECRET.
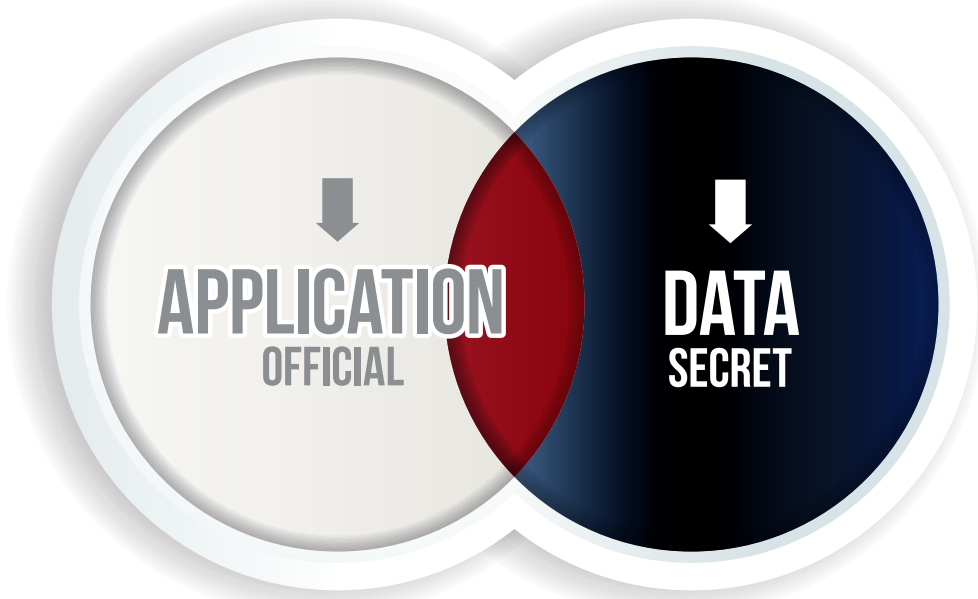
CDHA revolutionises data security by seamlessly bridging trust boundaries. With robust encryption and secure data transfer, CDHA empowers organisations to confidently manage and process sensitive data across diverse security classifications.
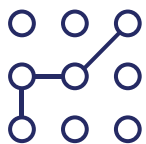
What is the CDHA Framework?

Secure by Design: A reusable pattern
for seamless cross domain collaboration

Acubed.it has designed this unique framework in collaboration with the National Cyber Security Centre (NCSC).
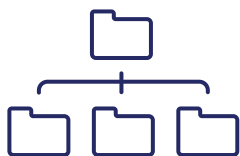
The Cross Domain Hybrid Application (CDHA) Framework is the only solution specifically designed to solve the complex cross domain application process.

Our approach is based on a zero-trust model and utilises the next generation high assurance gateway.

We provide a set of design patterns, a reference architecture, code libraries and guidelines.

Patterns   **Architecture**   **Libraries**   **Guidelines**

It is built to meet 'Secure by Design' principles and will help customer applications to also adhere to 'Secure by Default' principle.

The CDHA Framework provides a cryptographic key management system to solve the complex cross domain data and application security problem.

Using the CDHA Framework to Modernise Government Security

The implementation of zero trust architecture has introduced a paradigm shift to government's approach to network security. In contrast to the perimeter-centric threat model, zero trust architecture focus on the inherent qualities of the data.

As government modernises its approach to security, the Cross Domain Hybrid Application Framework provides an opportunity for a further step change. The CDHA framework is a new application design framework, which employs secure design methods to enable an application to communicate across security boundaries.

With 'secure by design' being the focus of the framework, we have produced a truly remarkable tool for enabling systems to talk to each other in a secure and safe manner.

Using Elliptic Curve Cryptography (ECC) technology, the data is secured by the user's own key pairs and sent to a higher trust location with validation and consistency checking at each stage of the journey.

The CDHA framework allows an application in a lower trust environment to collect data from a user but does not have the ability to access the data itself, ensuring that it does not become a point of failure or target for malicious activity.

When do you use the CDHA Framework?

- Users enter information into a form within the OFFICIAL or Low Trust domains, and the data is securely transferred to the High Trust area, leaving little to no trace behind.

- If your Low Trust application portal collects information at the OFFICIAL level and a segment of this data requires processing on a more secure network, then it's imperative to have the right protocols.

- If your application portal operates on a Low Trust domain and gathers data at the OFFICIAL level, that data must remain encrypted and protected at all times.
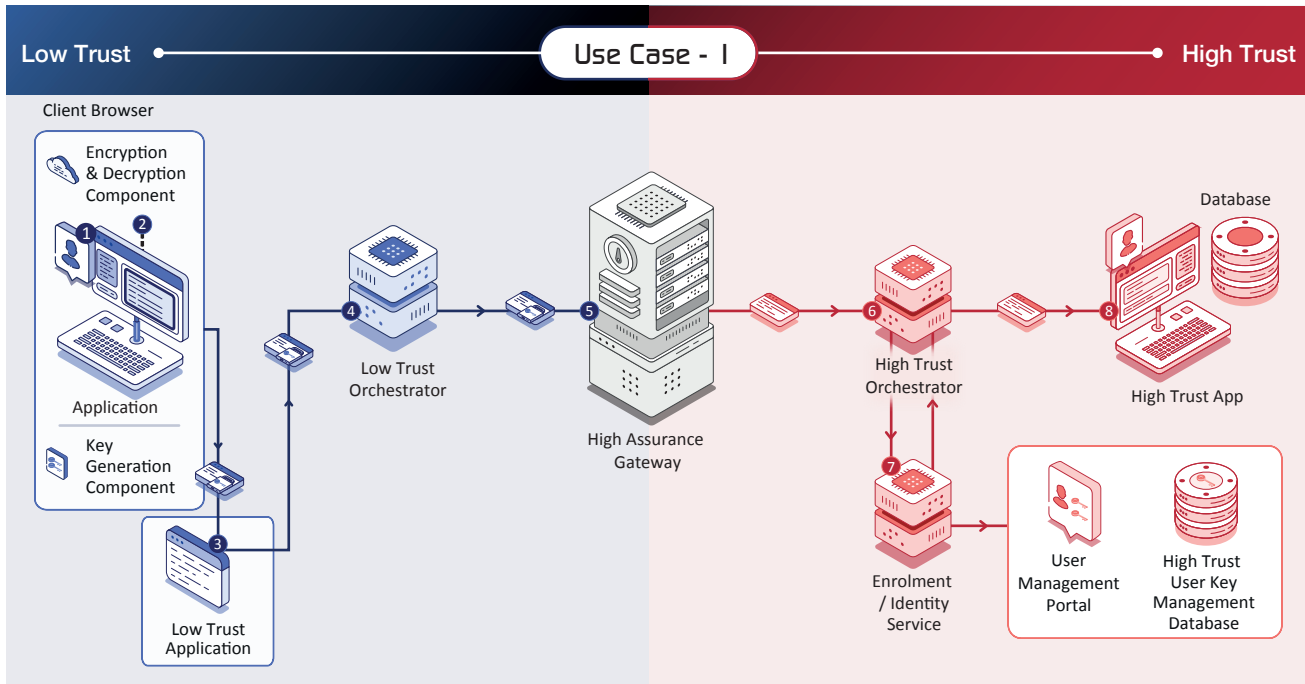
- While data may reside in the higher security tier, specific portions of records or data should be securely made available to the OFFICIAL level to enhance application accessibility.

There are numerous use case across HMG where the CDHA Framework can help solve the complex cross domain problem.

Use Case 1

Data securely collected at low trust then safeguarded at high trust with CDHA.

Low Trust — Use Case - 1 — **High Trust**

Client Browser
- Encryption & Decryption Component
- Application
- Key Generation Component
- Low Trust Application
- Low Trust Orchestrator
- High Assurance Gateway
- High Trust Orchestrator
- High Trust App
- Database
- Enrolment / Identity Service
- User Management Portal
- High Trust User Key Management Database
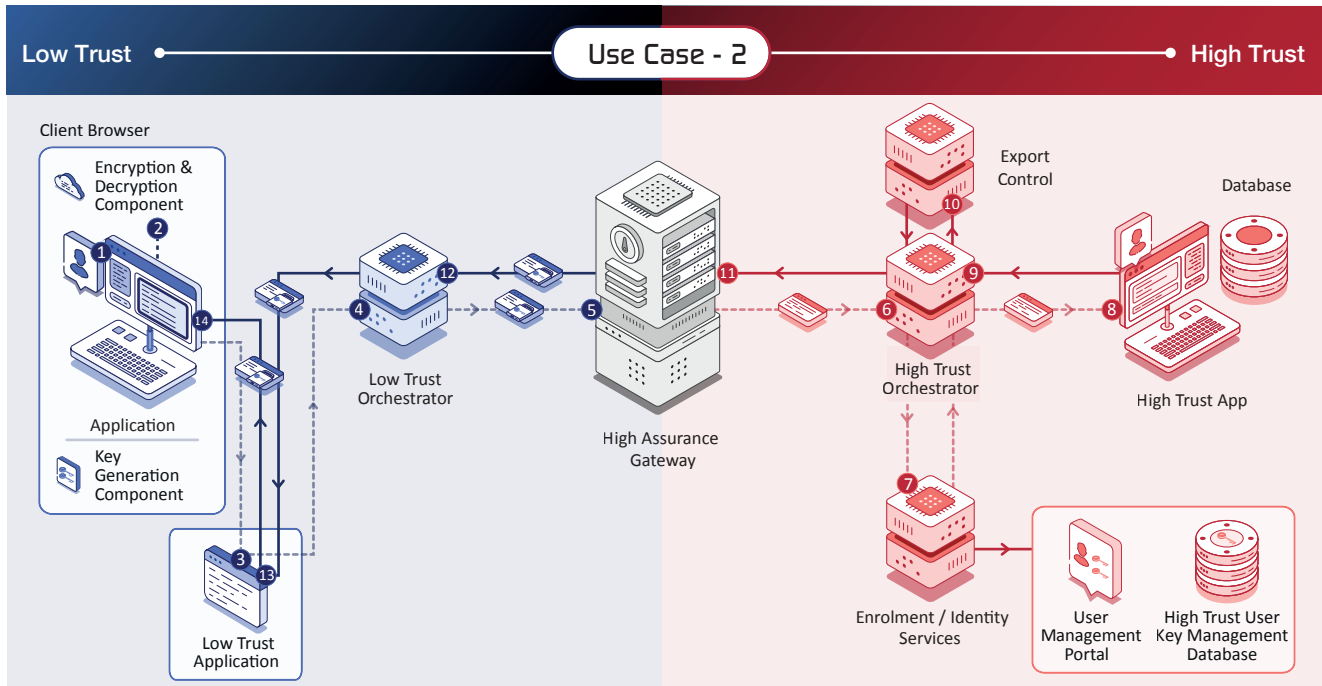
Application Needs

- Application has no data storage on the OFFICIAL tier.

- It's based on a fire and forget principal.

- This usually is applicable where users just need to submit some data.

- Most of the processing is done on the High Trust.

CDHA Features

- Data encrypted using the Browser based User's key.

- Only user holding the private key can decrypt the record on Low Trust.

- Each Application user will have its own Key Pairs.

- CDHA works on the Zero Trust principal which means every stage has digital signature verification for repudiation.

Use Case 2

Data securely collected at low trust and safeguarded at high trust whilst allowing seamless data retrieval & update.
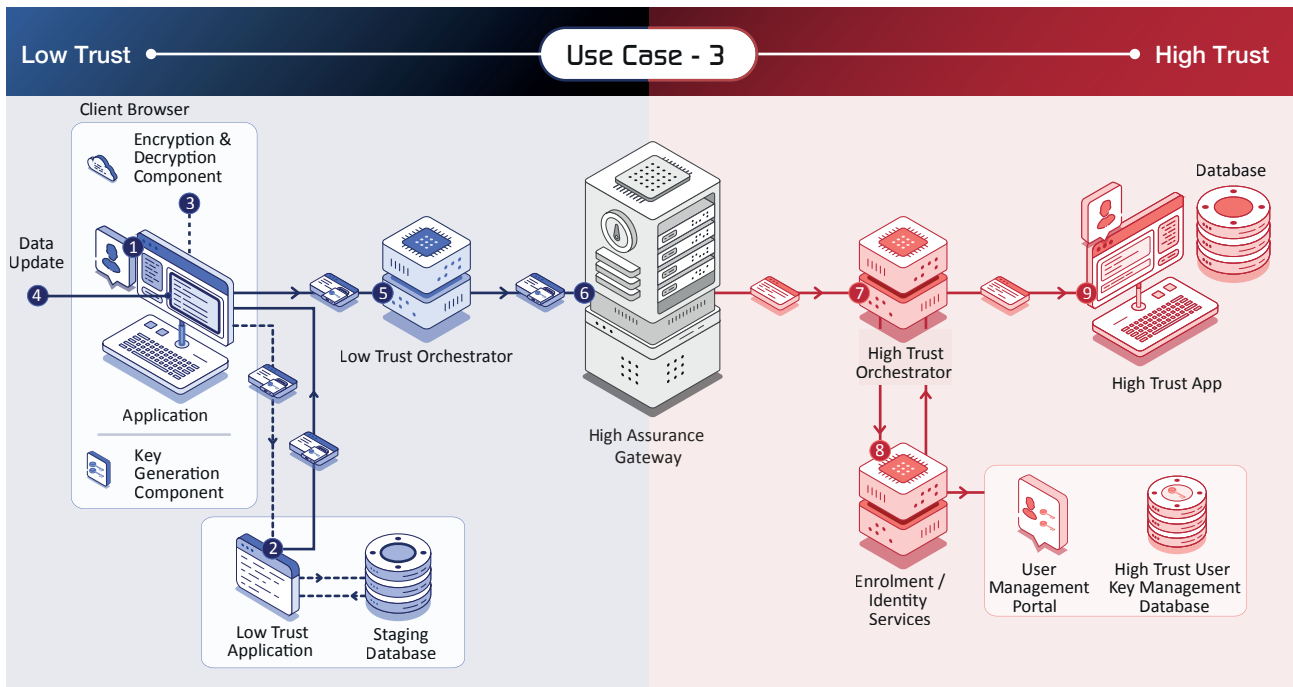

Application Needs

- Application has no data storage on the OFFICIAL Tier.

- This usually is applicable where users need to submit data which can take longer than 1 session.

- User needs to be able to retrieve their own data for further updates.

- User needs to be able to update and save the data.

- Most of the processing is done on the High Trust.

CDHA Features

- Data encrypted using the Browser based User's key.

- Only the user holding the private key can decrypt the record on Low Trust.

- When the user retrieves data, the High Trust goes through an export control mechanism to validate if data can travel to the Low Trust.

- Data is encrypted for the target users, and only the users holding the private key will be able to decrypt the data.

- Each application user will have their own Key Pairs.

- CDHA works on the Zero Trust principal which means every stage has digital signature verification for repudiation.

Use Case 3

Data securely collected and processed at low trust, then transferred to high trust for additional processing and fortified storage.
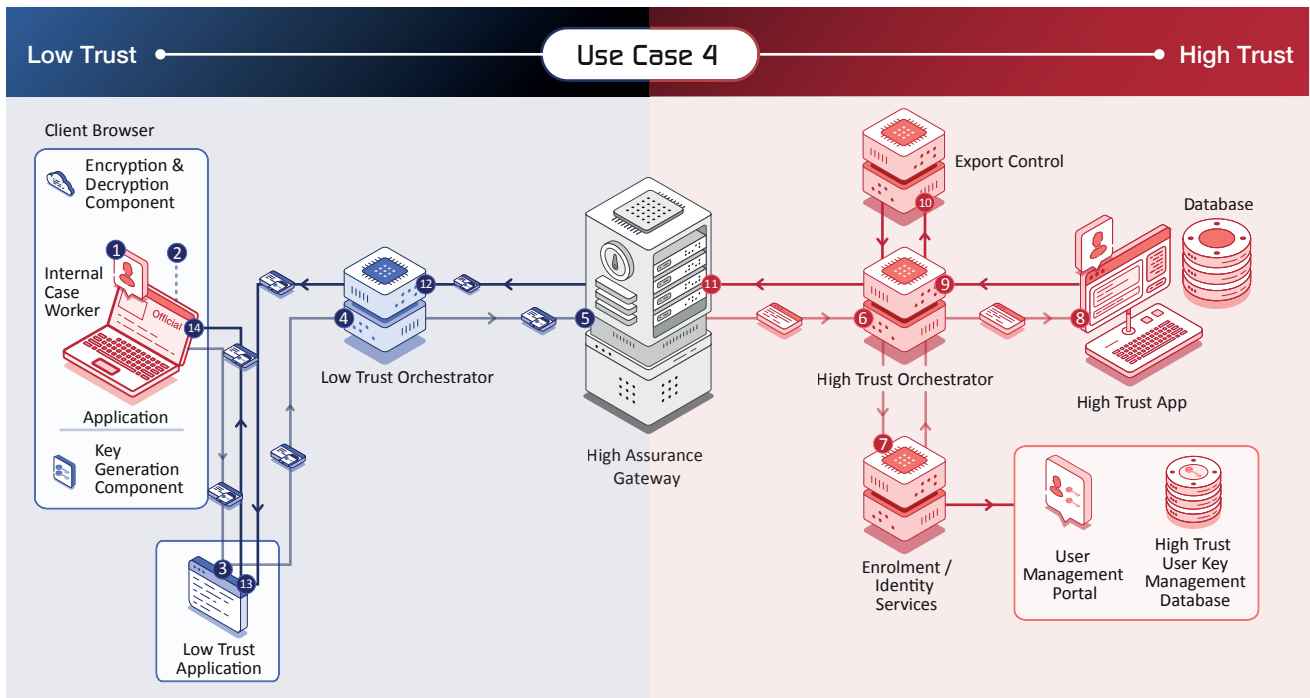

Application Needs

- Application has high volume transactions and needs to store the staging data at OFFICIAL securely.

- This usually is applicable where users need to submit data which can take longer than 1 session.

- User needs to be able to retrieve own data for further updates.

- User needs to be able to update and save the data.

- Once user submits the data, it needs to move to the High Trust for storage and further processing.

- Most of the processing is done on the High Trust.

CDHA features

- Data encrypted using the Browser based User's key.

- Only user holding the private key can decrypt the record on Low Trust.

- Data is encrypted for target users and only the users holding the private key will be able to decrypt the data.

- Each Application user will have its own Key Pairs.

- CDHA works on the Zero Trust principal which means every stage has digital signature verification for repudiation.

- Once submitted, data will travel from the browser session to the High Trust using a combination of users and High Assurance Gateway (HAG) key.

Use Case 4

Data is securely stored in high trust, where internal users retrieve official records and process using OFFICIAL EUD.

Low Trust ● ——— **Use Case 4** ——— ● **High Trust**

Client Browser
- Encryption & Decryption Component
- Internal Case Worker
- Application
- Key Generation Component
- Low Trust Orchestrator
- Low Trust Application
- High Assurance Gateway
- Export Control
- High Trust Orchestrator
- Database
- High Trust App
- Enrolment / Identity Services
- User Management Portal
- High Trust User Key Management Database

Application Needs

- Data is stored at the High Trust.

- Single record or part of the record is OFFICIAL.

- Internal case workers needs to access the data securely on OFFICIAL device.

- Only data which is classified as OFFICIAL should be able to travel to the Low Trust.

CDHA Features

- Data is encrypted for target users and only the users holding the private key will be able to decrypt the data.

- Each application user will have its own Key Pairs.

- CDHA works on the Zero Trust principal which means every stage has digital signature verification for repudiation.

- System only releases OFFICIAL data when requested from the Low Trust. Everything going to the High Trust passes through an export control mechanism to control what gets released to OFFICIAL.

About Us

Acubed.IT works with UK Government Departments to assist with transforming the way HMG perform secure processes and data capture, enabling performance, delivering efficiency & enhanced data security.

Based in the UK, our team of expert's design, build and integrate powerful and highly secure digital solutions that automate and transform business processes.

Our company works collaboratively with HM Government Departments and Public Sector organisations to solve their most pivotal and technically complex security challenges.

We work with the NCSC (National Cyber Security Centre), and other government departments, supporting the research and development of vital innovative technologies and solutions.

We have in depth experience of working on the UK's cross-government official and higher tier platforms and have collaborated with the NCSC to develop the next generation CDHA Framework.
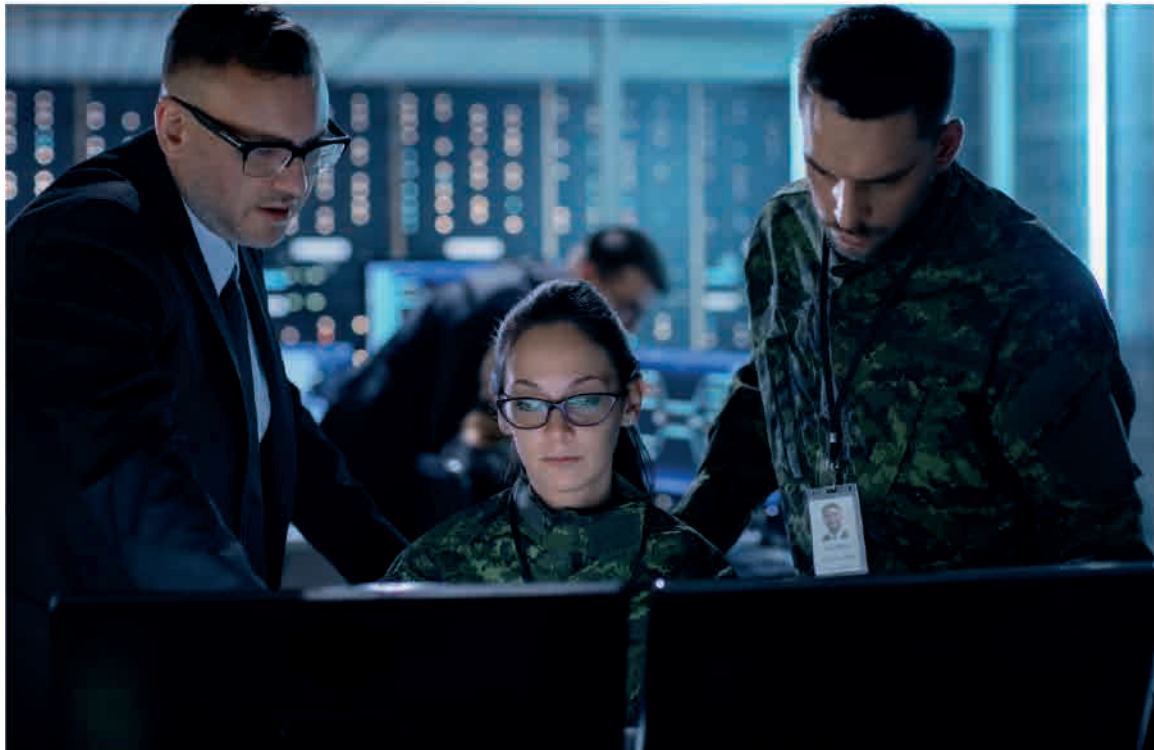
People Who Trust Acubed.IT

The Acubed.IT team works closely with its clients to provide cutting-edge customised solutions to ensure the ever-evolving cyber security of the UK is top priority.

Utilising industry leading technology, our cross domain and cloud specialist expertise, we are committed to working with our partners to take cyber security solutions to a whole new level.

Benefits of CDHA Framework

The Cross Domain Hybrid Architecture (CDHA) framework, developed by Acubed.it in collaboration with the NCSC

CDHA Benefits

Cross Domain Crypt Keys Management

Our solution is unique and has no direct competitors.

Secure Data Transfer

Secure movement of data between High and Low Trust environments.

Data Storage at Secret

Aggregated data stored in a secure domain.

Seamless User Key Management

Our Solution enables a seamless experience of key management for the end user.

Reduces the need for Secret EUD

Significantly reduces the need for T2 End User Devices and infrastructure.

Next Generation Cross Domain Solution

CDHA Protects against the highest threats, protecting the UK's most sensitive systems.

acubed.it
Designing Secure Applications

Concerned about data aggregation risks on the low side?

We can provide:

- **CDHA Libraries and Guidelines (Licence only)**
- **Architecture Support for CDHA capabilities**
- **CDHA & Security Consultancy for designing your application exploiting CDHA capabilities**
- **Design and build Application aligned with CDHA guidelines**

Talk to us now about the CDHA framework and how it can help your deployments and cross domain needs.

✉   enquiries@acubed.it

🌐   www.acubed.it

in   www.linkedin.com/company/acubed-it

Exciting News!

Acubed.it is working in collaboration with Cross Domain Gateway and Processor Innovation organisations to bring CDHA capabilities to the Private Sector.

intel.
#becrypt

CYBER ESSENTIALS CERTIFIED PLUS

JOSCAR REGISTERED

Citation ISO Certification
Information security management
ISO 27001: 2022
REGISTERED
Certificate No 448902024

Crown Commercial Service Supplier

MENTAL HEALTH AT WORK COMMITMENT

Carbon Literacy Project

A company registered in the UK, company registration number No.12285965