# Cross Domain Hybrid Application Framework

**A reusable pattern for seamless interoperability & cross-domain collaboration**

acubed.it
Designing Secure Applications

# The Problem

## Cross-domain working is a key challenge area for the National Cyber Security Centre (NCSC)

As national security threats evolve, data silos and fragmented security domains create operational inefficiencies and elevate security and compliance risks. These challenges are further compounded by two critical issues:

- **Data Aggregation Risks** - Unprotected sensitive data at the OFFICIAL classification is a prime target for Hostile State Actors.
- **Restricted Visibility & Access:** Isolated SECRET systems, limit operational agility and cross-domain collaboration.

To mitigate these risks, appropriate security measures must be implemented, enabling secure interoperability.

### Example Use Cases

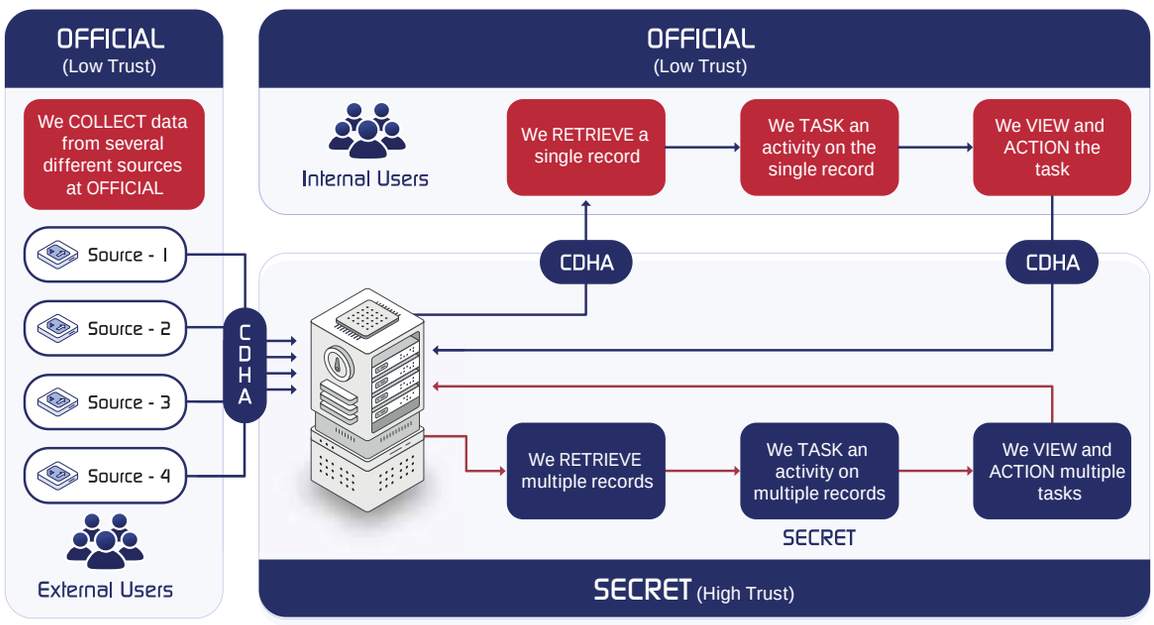
1. **Vetting Process**
2. **NIS Data**
3. **CAF Documents**
4. **Cross-Domain Collaboration and Intelligence Sharing**
5. **Government and Law Enforcement**
6. **Secure Identity Management & Access Control**

# The Solution

## Cross Domain Hybrid Application (CDHA) Framework – Enabling Secure Interoperability Across Security Domains

With increasing regulatory pressure from NIS2, CAF, and the Cyber Resilience Bill, organisations must adopt solutions that go beyond basic data transfer – they need operational efficiency, cryptographic security and seamless cross-domain application functionality.

CDHA is a next-generation approach – a secure application framework designed to address these challenges. It enables data protection across all classification levels, mitigating data aggregation risks at OFFICIAL and enabling authorised access to SECRET environments without compromising security.



# What is the CDHA Framework?

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

Acubed IT, in collaboration with the NCSC, has developed the Cross Domain Hybrid Application (CDHA) Framework - a unique solution designed to address the challenges of cross-domain application development.

Built on a zero-trust model and leveraging next-generation high-assurance gateway technology, the CDHA Framework offers a comprehensive suite of design patterns, a reference architecture, code libraries, and implementation guidelines.

Patterns | Architecture | Libraries | Guidelines

Built to facilitate Secure by Design principles, the CDHA Framework also helps ensure customer applications align with Secure by Default standards, while incorporating an advanced cryptographic key management system to address the complex security requirements of cross-domain applications.

# Future-Proof Security with Post-Quantum Innovation

As quantum computing threatens traditional encryption, Acubed IT, in collaboration with Edinburgh Napier University, is integrating **Post-Quantum Cryptography (PQC)** into the CDHA Framework to ensure enduring data protection.

Key Innovations Include:

- **ML-KEM and ML-DSA Algorithms:** Strengthening encryption against quantum-based threats.
- **Homomorphic Encryption (HE):** Enabling secure computations on encrypted data without decryption.
- **Attribute-Based Encryption (ABE):** Allowing controlled data sharing across domains based on user roles and security clearances.
- **AI & ML-Driven Export Controls:** Automating compliance and security checks for cross-domain transfers.

Together, these innovations will reinforce CDHA's long-term security and resilience against emerging cyber threats.

# How does the CDHA Framework differ from Cross Domain Solutions (CDS)?

**CDHA is more than just another Cross Domain Solution** - it represents the next generation of secure applications, bridging the gap between security and usability to enabling data-driven decision-making while safeguarding critical information.

1. **Data Protection at the OFFICIAL domain** - CDS primarily protects the SECRET network but does not protect data at the OFFICIAL domain. CDHA encrypts data from the moment of creation, ensuring protection before it moves to higher domains.
2. **Operational Efficiency** - With CDS, users must manually move data to higher domains. CDHA allows secure data processing at lower classifications while keeping aggregation at higher domains - reducing duplication, manual work, and inefficiencies.
3. **Secure Access to SECRET Data from OFFICIAL Devices** - In CDS environments, higher domain data is often inaccessible from OFFICIAL systems. CDHA allows secure, controlled access to portions of higher domain data from OFFICIAL devices, ensuring real-time decision-making without compromising security.
4. **Future-Proof Cryptography** - While CDS relies on legacy security models, CDHA integrates Post-Quantum Cryptography (PQC), Attribute-Based Encryption (ABE), and Fully Homomorphic Encryption (FHE), ensuring long-term security against evolving threats.

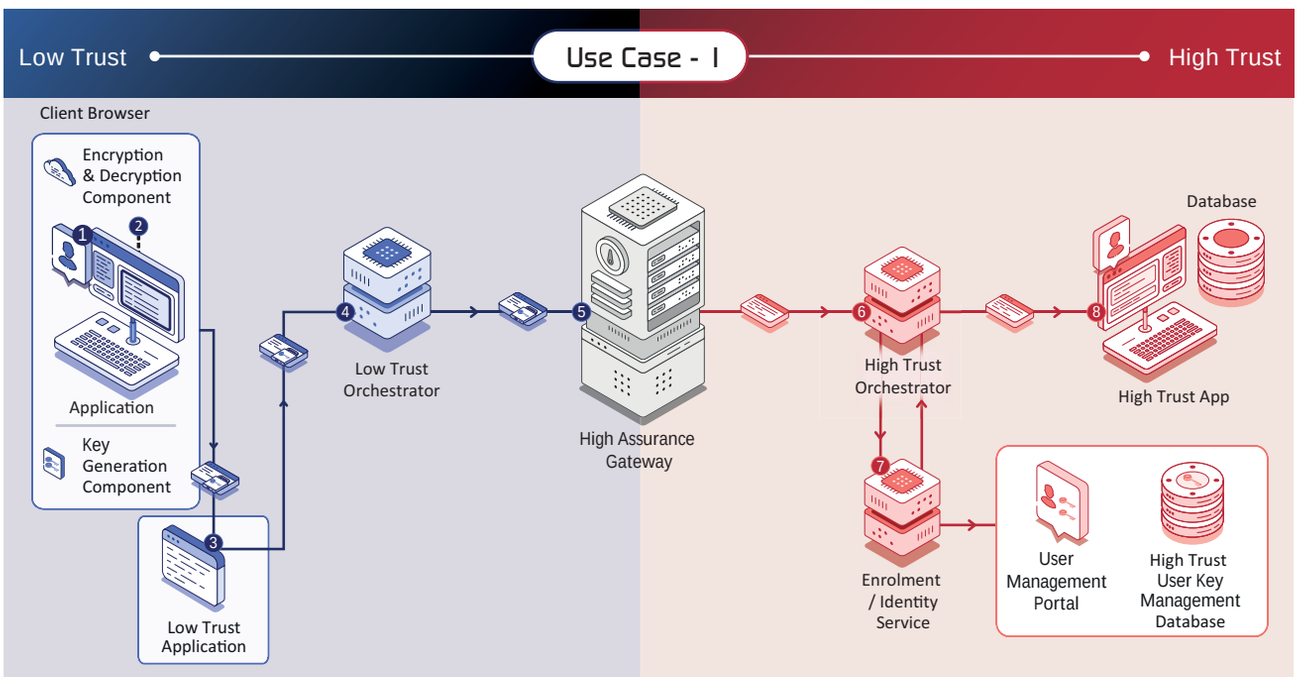
# When do you use the CDHA Framework?

- 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 cases 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.




## Application Needs

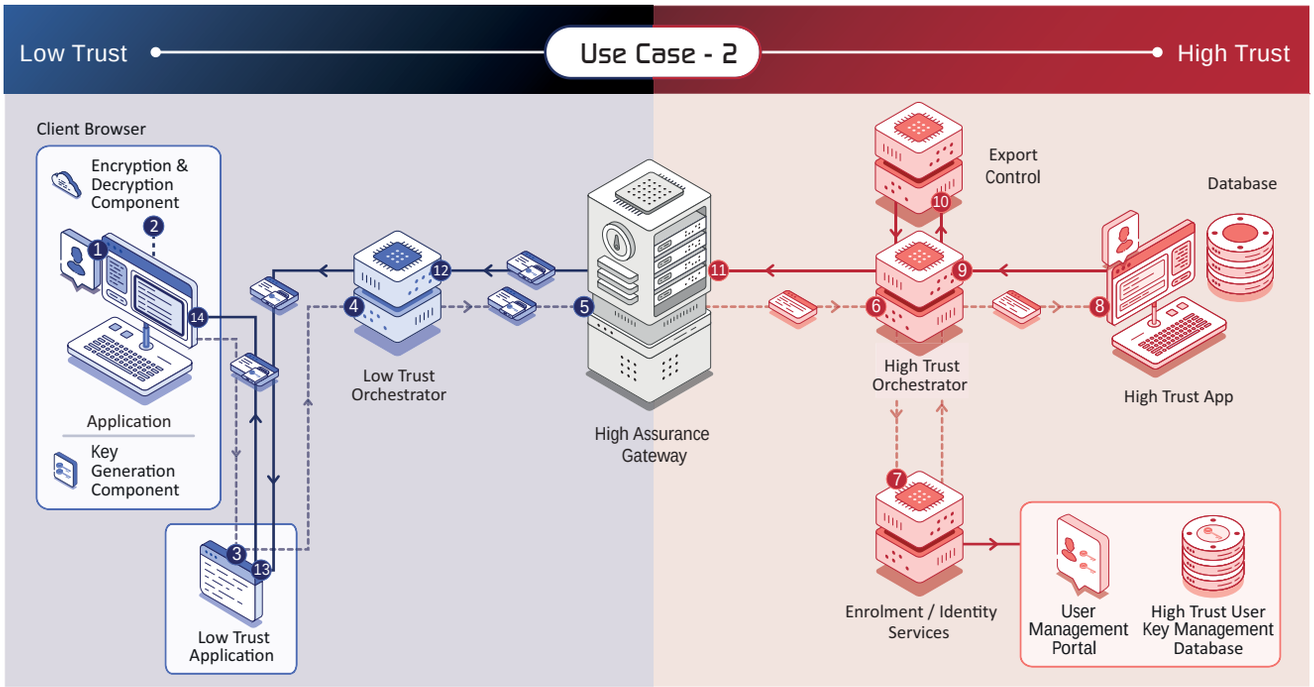
- **Application has no data storage on the OFFICIAL tier.**
- **It's based on a fire and forget principal.**
- **This usually is applicable where users just need to submit some data.**
- **Most of the processing is done on the High Trust.**

## 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

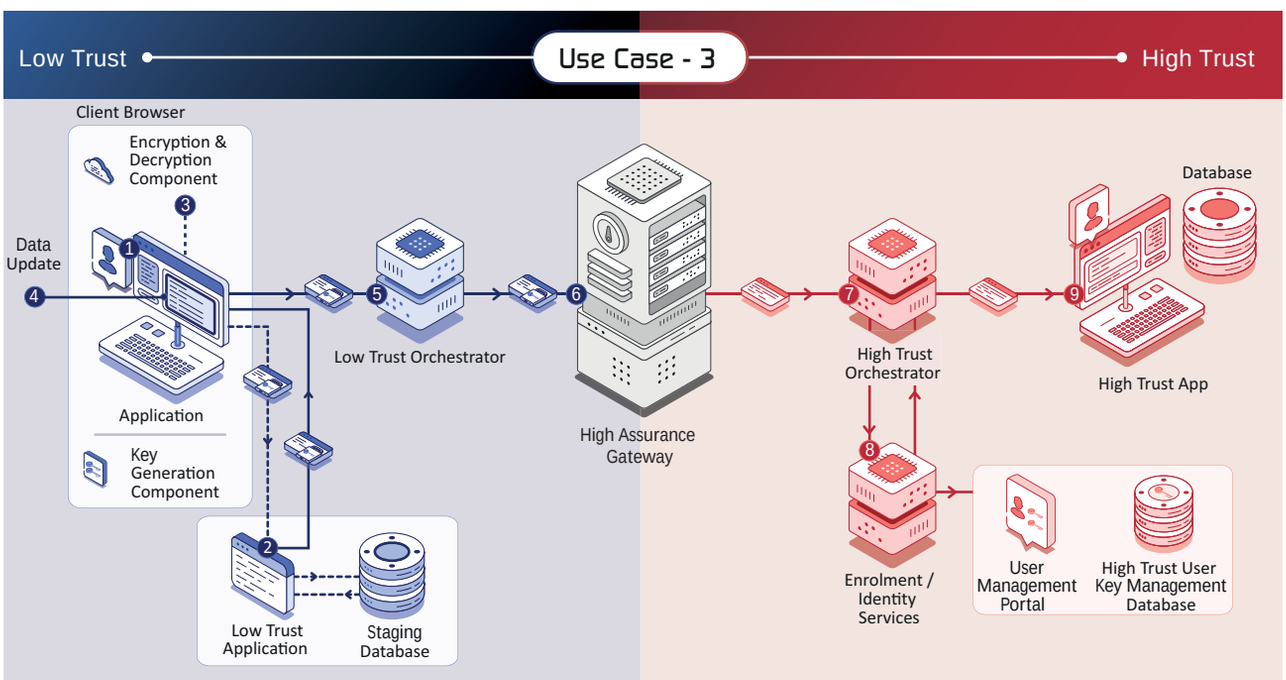
- **Application has no data storage on the OFFICIAL Tier.**
- **This usually is applicable where users need to submit data which can take longer than 1 session.**
- **User needs to be able to retrieve their own data for further updates.**
- **User needs to be able to update and save the data.**
- **Most 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

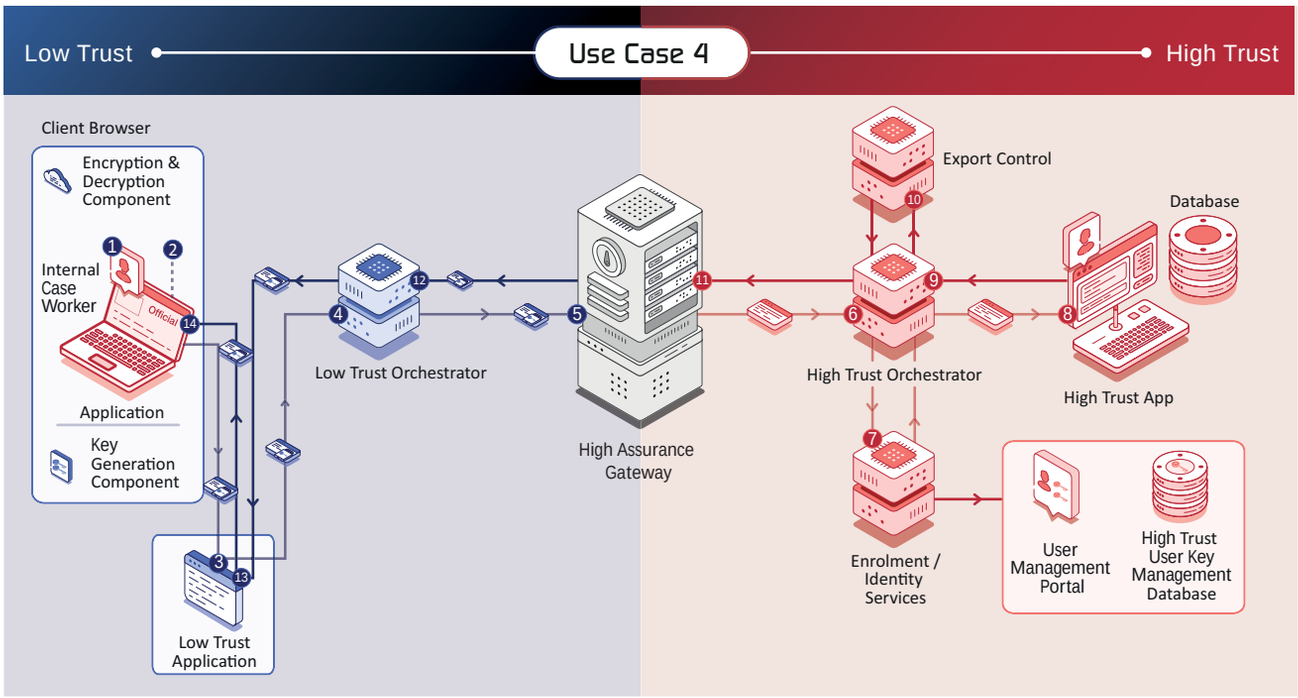
- **Application has high volume transactions and needs to store the staging data at OFFICIAL securely.**
- **This usually is applicable where users need to submit data which can take longer than 1 session.**
- **User needs to be able to retrieve own data for further updates.**
- **User needs to be able 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.




## 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.**

# Enhancing CNI Protection with Advanced Cross-Domain Solutions

**Cross Domain Hybrid Application Framework (CDHA) is designed to secure Critical National Infrastructure (CNI) against emerging cyber threats. As Europe transitions to new regulatory frameworks like NIS2 and the UK prepares to enact its own Cyber Security and Resilience Bill, CDHA offers a proactive solution to meet and exceed compliance and security expectations for data handling.**

**Robust Encryption for CNI Protection:** CDHA utilises well recognised and accepted cryptography schemes to safeguard sensitive CNI data, ensuring that critical information remains protected from unauthorised access, while in transit and at rest. This aligns with the anticipated requirements of the UK's forthcoming **Cyber Security and Resilience Bill**, which prioritises the safeguarding of CNI data.

**Secure Information Sharing Between Regulators and Operators of Essential Services (OES):** Facilitate secure and efficient data sharing between different organisational entities, from operators to regulators. CDHA ensures that any shared information adheres to high-trust protocols, crucial for maintaining the integrity and confidentiality of CNI-related communications.

**Compliance and Adaptability:** As the Cyber Security and Resilience Bill moves from consultation to enforcement, CDHA provides a Secure Cross Domain Framework that helps organisations stay compliant with new and evolving cybersecurity laws.

**Operational Efficiency and Regulatory Compliance:** Beyond securing data, CDHA enhances operational efficiencies through streamlined data handling and reduced complexity in cross-domain interactions. This not only boosts performance but also simplifies the compliance process for entities governed under strict regulatory mandates.

**Conclusion:** As the Cyber Security and Resilience Bill shapes the future landscape of cybersecurity in the UK, CDHA Framework is designed to meet these challenges head-on. Protect your critical assets with a framework built for the future of CNI protection, ensuring your operations are secure, compliant, and resilient.

# Benefits of CDHA Framework

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

### Cross Domain Crypto Keys Management

Our solution is unique and has no direct competitors.

### Reduces Risk of Data Breaches

Protects sensitive date even before it reaches higher classifications.

### 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.

### Improves Operational Efficiency

Eliminates security bottlenecks by enabling secure data interoperability

# About Us

At Acubed IT, we design and deliver secure, scalable, and innovative technology solutions across the National Security, Defence, and Public Sector ecosystems. Leveraging deep expertise in sensitive domains and cryptography, we are advancing the future of secure application development.

## At a Glance:

- All staff hold SC/DV level National Security Vetting
- Deep-tech team with real-world defence project experience
- Active collaborations with UK Government, Defence Primes and Academia

# The Acubed Advantage: Why Choose Us?

Acubed IT specialises in designing and implementing Next-Generation Secure Applications built on the CDHA Framework. Our expertise in cross-domain security and secure application development enables us to tackle complex data security challenges that others can not address.

Having worked in collaboration with the NCSC on the CDHA Framework development, we bring extensive technical knowledge and practical insight into how CDHA can be effectively applied to real-world use cases. This experience enables us to design and develop secure applications that seamlessly integrate across security classifications, providing robust data protection, operational efficiency, and compliance with evolving security regulations.

With a proven track record in national security, defence and critical infrastructure, Acubed IT is dedicated to driving secure digital transformation through innovative, scalable, and resilient solutions.

# Some of Our Clients & Partners

Foreign, Commonwealth & Development Office

Home Office

Cabinet Office

Department for Business, Energy & Industrial Strategy

Government Property Agency

HM Revenue & Customs

Ministry of Defence

METROPOLITAN POLICE

Telefónica Tech

#becrypt

acubed.it
Designing Secure Applications

# Are you concerned about Data Aggregation at OFFICIAL?

**We offer:**

- **Application Design and Development** following CDHA guidelines
- **Architecture Support** for CDHA capabilities
- **Access to CDHA** Libraries and Guidelines (Licence Only)
- **CDHA and Security Consulting** to help design applications that fully leverage CDHA capabilities

# Contact Us

Talk to us today about the CDHA Framework and how it can support your deployments and cross-domain needs.


CDHA@acubed.it

www.acubed.it

www.linkedin.com/company/acubed-it


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

Citation ISO Certification Quality management ISO 9001 REGISTERED
Certificate No:448902024

Citation ISO Certification Environmental management ISO 14001: 2015 REGISTERED

CYBER ESSENTIALS CERTIFIED PLUS

JAMES CYBER ASSURANCE

QUALITY PRINCIPLES

Assured Services Provider
In association with National Cyber Security Centre
Cyber Advisor (Cyber Essentials)

JOSCAR REGISTERED

Crown Commercial Service Supplier

National Cyber Security Centre For Startups Alumni

CYBER RUNWAY ALUMNI

# Exciting News!

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


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