Our Experience

Defence and Intelligence agencies

Cogito Group consultants have primarily worked for the Australian Defence Organisation (ADO) and Intelligence agencies, both domestically and overseas.

Cogito Group have a proven track record delivering the largest and most geographically dispersed smartcard implementation in Australia for the ADO, issuing over 2 million soft and hard token certificates in its lifetime. This implementation also has some of the harshest environmental and industrial conditions that can be imagined including sea, cold, hot, humid and dusty conditions and with staff that put smartcards under heavy physical stress as well. This rollout not only required distributed registration and use across Australia, but also encompassed deployments overseas. These services were also required to secure high level access to trophy systems containing highly classified information.

> Cogito Group has a proven track record of delivering the largest and most geographically dispersed smartcard implementation in Australia.

Card Management Systems

Cogito Group designed, built, tested and sustains three complete Card Management Systems for the ADO.

Cogito designed and built the Card Management Systems to:

- Support personnel located internationally with registration points located in major capital cities across Australia, allowing the 120,000+ Personnel to have close access to a registration point to receive a smart card.
- Issue smartcards from a central location using batch processing to reduce operational costs and complexity, and to maintain higher security over card stock and card keys.
- Issue smartcards with both LACS and PACS capabilities.
- Issue smartcards with certificates that are Gatekeeper (AGIMO) certified.
- Support multiple smartcard types.
- Be deployed on a classified network for issuance of smartcards used to access Australia's Allies ICT systems.

The original implementation continues to expand. The initial 3,000 licenses is planned to increase and roll-out to all administrators on multiple networks is now being completed.

Sustainment

Cogito Group have provided continual sustainment of these CMS solutions for the past 4 years (and are contracted for another 3 years). This sustainment work includes:

- Resolution of issues & bugs that arise with the products.
- Identification and Implementation of Enhancements to the processes and products.
- Training to standard users, operators and system administrators.
- Engagement with groups internal to ADO to help enable more capability for Smartcards.
- Operation, engineering and maintenance support.

Cogito Group provide other software services that include design, development, testing, build, deployment, implementation, data migration, integration training, maintenance, configuration and support.

Security Management

Public Key Infrastructure (PKI)

Cogito Group provided the installation, integration and testing services to a new facility to allow the joining and access of other networks to the Australian Defence Organisation's environment at the Highly Protected network level.

Multi-factor Authentication (MFA)

Cogito Group provided an MFA end to end solution. This required new services and systems to be installed for the pass-through of information and inspection of that information without interrupting the dataflow. Cogito Group installed and configured the infrastructure to be used to achieve this.

Digital Signing

Cogito Group have delivered new approval processes to migrate manual processes into ITIL compliant software platforms. In addition, Cogito have PKI-enabled the organisation, paving the way for approval processes to become digitised with digital signing instead of wet-ink signatures, cutting down manual document handling, physical document management costs, creating a paperless society.
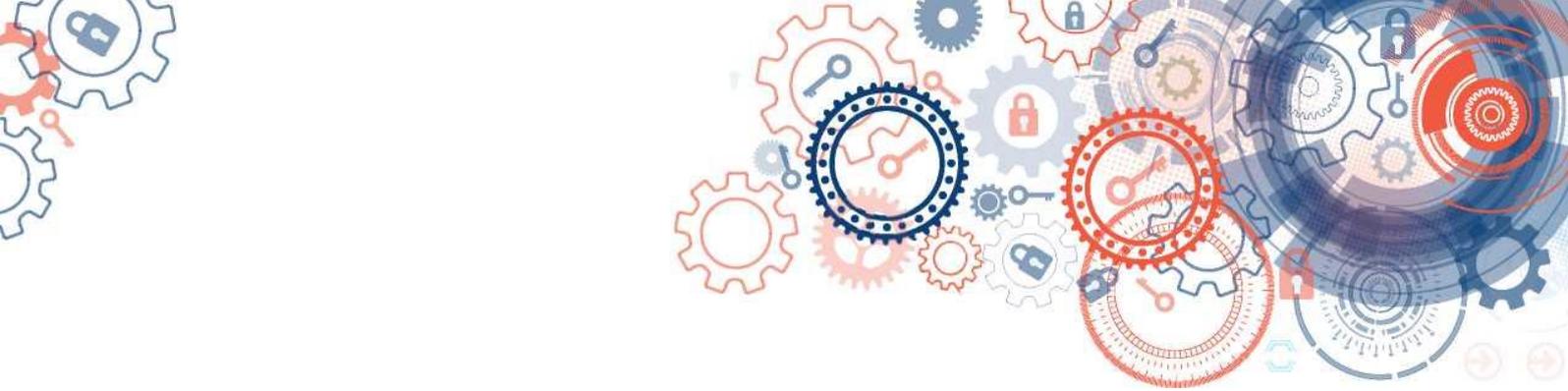
Security Strategy

Gatekeeper Accredited CA

Cogito Group were contracted by the ADO to assist with development of policy and documentation in their GateKeeper Accreditation, through the Australian Government Information Management Office (AGIMO – Department of Finance).

Cogito Group is in the process of gaining Gatekeeper Accreditation this requires compliance with the ISM and PSPF. Cogito has developed (and submitted) the requisite strategy to be employed to maintain the integrity and confidentiality required in a solution that actually provides those services to other systems. Cogito already has in place the plans and architectures to meet the ISM and PSPF requirements to the level of Highly Protected.

Cross Certification

As part of interoperability between the ADO and its allies, Cogito Group have been integral in development and negotiation of PKI Interoperability agreements between the United States Department of Defence (US DoD) and the ADO high and low networks. Cogito have ensured that future-proofing is maintained with the solutions, having been involved in the strategic planning including development and evaluation of the required solution and performed research and analysis of implementation methods and best practices. Cogito provided the key planning documentation and advice for management and governance frameworks such as the ACP 185.

End User Computing

Single Information Environment (SIE)

Cogito Group is currently implementing the Single Information Environment (SIE), a next-generation technology domain for allowing its client to move IT infrastructure to more cost effective virtual platforms. Cogito Group were engaged to provide replicas of the Corporate Directory, Public Key Infrastructure and Smartcard Management System to enable integration and testing of these existing components against the new SIE domain and its differing architecture and management infrastructure.

Cogito Group are engaged to provide key integration between key network resources, platforms and software between the old and new solutions. Both networks are required to interact with one another until the new solution reaches final operational capability.

Developing strategy that maintains integrity, availability, non-repudiation and confidentiality.
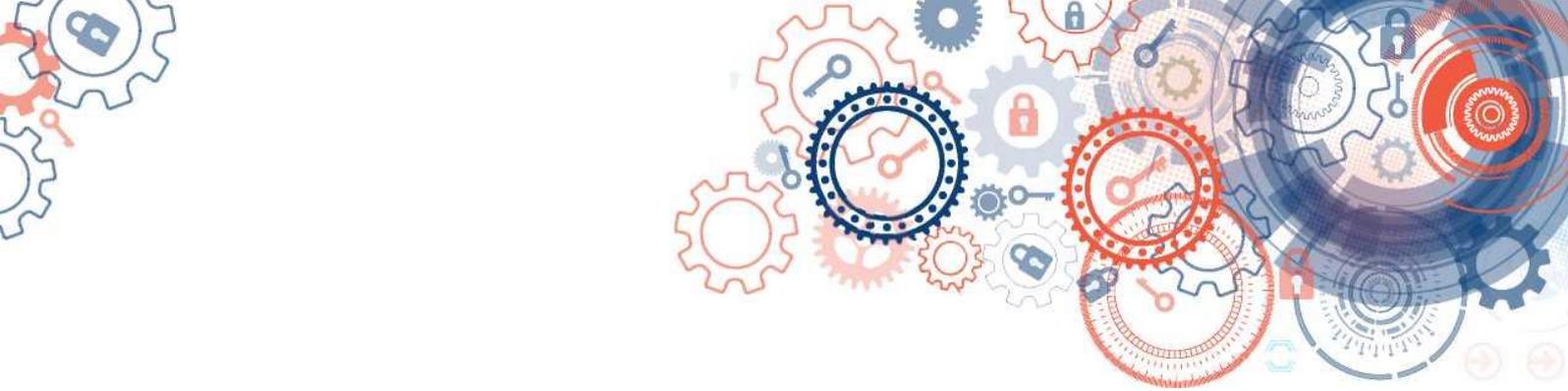
Security Solutions

HSM Upgrade

Cogito Group delivered the upgrade of all Australian Defence Organisation Hardware Security Modules (HSMs).

Web-based solutions

Cogito Group have delivered numerous web-based systems to Australian Defence Organisation, including Smartcard Management Systems, PKI Management Portals and General Information Sites. Cogito staff possess strong skills in various web platforms, including Java, ASP.NET, Node.js and Django.

Cogito Group possess staff with solid technical understandings of XML and XBRL (including XBRL Taxonomies), UI design and development, usability and accessibility testing, user traffic targeting and optimisation.

Integration Specialists

Cogito Group are experienced system integrators and specialise in bringing together component subsystems into a whole and ensuring those subsystems function together. We focus on bridging the common operational gaps faced in the integration of digital security technology. Our consultants have specialist knowledge in data synchronisation and manipulation between disparate systems.

Cogito Group were engaged by the Australian Defence Aircraft Maintenance Environment (AME) to provide PKI Enablement of WIFI-enabled devices to secure communication channels. Cogito successfully delivered this capability, integrating both the AME's enrolment application architecture with the existing PKI application architecture, allowing for both group's architectural needs to be maintained and operability to continue with little intervention required.

Cogito ensured that the business logic, delivery channels and data management contained within the device credential issuance process would be kept as the standard processes provided by the Operating Systems used, thus providing assurance that future enhancements would cause only minor integration issues.

Cogito developed, as part of the AME work, a template and delivery channels for provisioning WIFI into separate domains that has now been used numerous other times within the ADO.

As part of the wider use of PKI, Cogito staff integrated auto enrolment of digital certificates across the Protected and Secret Networks. This rollout was extended to include soft certificates for all users within these networks. This system has now been running successfully for a number of years and has been extended to other smaller connected networks such as the Defence Science and Technology Organisation's network.

To date over 2 million digital certificates have been issued from this facility. Cogito has been instrumental not only in the implementation of this solution, but also the use and management of these certificates over time. The certificates for this service are now used for such diverse uses as digitally signing documents for personnel appraisals and procurement approvals as well as the signing of emails.

> We focus on bridging the common operational gaps faced in the integration of digital security technology.

Security Policy

Cogito Group is experienced in creating and assisting with the development of IT Security strategy, plans, architecture, solutions and services that maintain the confidentiality, integrity and availability of IT systems, information and data. This includes developing strategies, conducting security audits and identifying risk areas to ensure compliance with policy and standards.

Cogito provides these services in accordance with the Australian Government Information and Security Manual (ISM), the Protective Security Policy Framework (PSPF) and ISO 27001 Information Security Management.

Our clients are ISO 27001 certified and compliant, and as such, all work that Cogito Group delivers is required to meet this requirement as well as the requirements of the ISM and PSPF.

Through the multiple projects and third level support services with the ADO, Cogito has assisted with the development of the ADO IT Security Strategy. Cogito has also delivered detailed plans, architecture, solutions and services for their PKI which provides the confidentiality, integrity, non-repudiation and availability of its IT systems.

Cogito has developed (and submitted) the requisite strategy to be employed to maintain the integrity and confidentiality required in a solution that actually provides those services to other systems. Cogito already has in place the plans and architectures to meet the ISM and PSPF requirements to the level of Protected.

This level of skill and knowledge with IT security policy, standards and technical instructions was first demonstrated many years ago when Cogito staff achieved the first High Assurance PKI accreditation in Australia for the ADO. Post the implementation of the ADO solution, Cogito has been involved in and conducted security audits in order to ensure that the independent audits required by the Gatekeeper process go as smoothly as possible and that adverse findings are ideally non-existent or kept to a minimum.

> Cogito develops strategies, conducts security audits and identifies risk areas to ensure compliance with policy and standards.
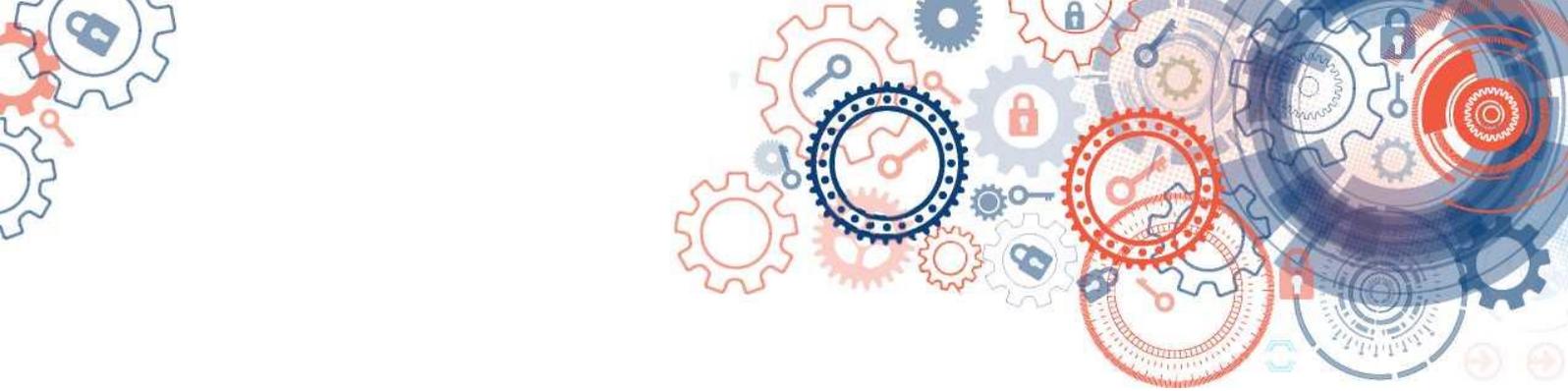
About Cogito Group

Cogito Group is an award winning Australian owned and operated ICT company specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.