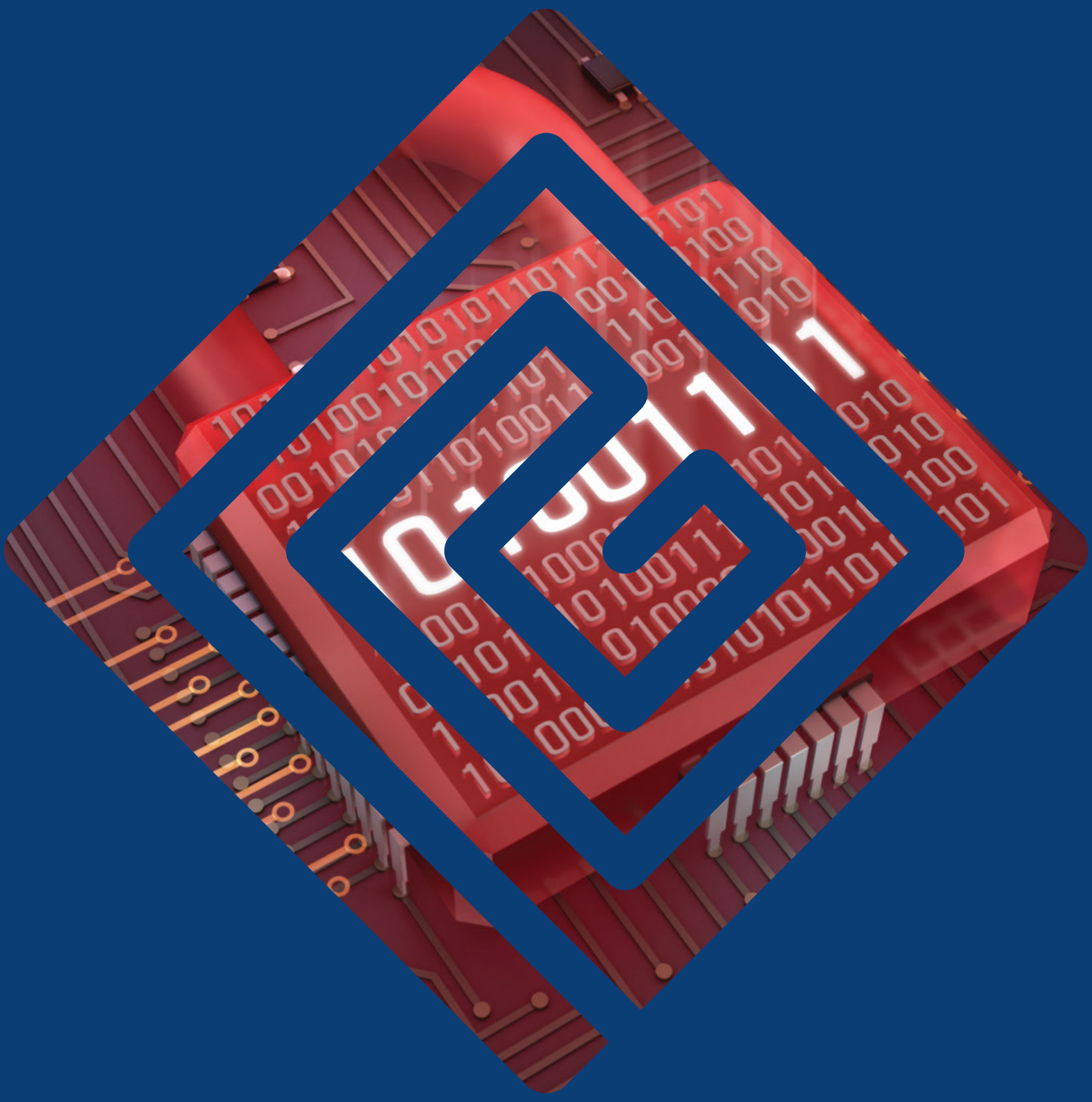
Cogito Group

Future proof your IT security foundations with enabling technologies.

Establish the four pillars for cyber security

Non-repudiation | Authentication | Integrity | Confidentiality



THE ISSUES

Will your security needs be met as new threats, devices and users needs evolve?

Today's cybersecurity threats are becoming more and more sophisticated. Each day we read news of cyber security breaches that highlights the intensifying magnitude of execution.

In a rapidly changing landscape, the trusted insider threat (Snowden) and Bring Your Own Device (BYOD) are but two examples that highlight a comprehensive, layered approach to security and authentication is essential.

Coupled with these factors, the post Sept 11 environment has led to the need for increased interoperability, sharing and collaboration between government agencies and allies. As we actively invite 'guests' into our organisation it's more important than ever that we maintain control over who they are (identity) and their access rights to the information.

It's a complicated scenario. We've witnessed the growth of the internet and the ever increasing connectivity of people and devices; dynamic intelligence over static intelligence and the borderless over the perimeter.

These days we need to adapt to internet scale rather than enterprise scale.

Our systems are no longer just on our physical premises, but in the cloud and accessible via the internet – and they are accessed any time, day or night from anywhere in the world. They are accessed not only by employees but contractors, customers and partners. In the not so distant past, you needed to physically carry hardware out of a building to steal information.

These days with virtualization, a server can be stolen remotely, simply as a file or accessed and altered in a malicious way.

This all adds up to requiring security solutions that are adaptable, scalable and integrated. We need to be able to provide flexible services to meet the operational tempo. They need to be managed in a way that combines encryption, access policies, key management, content security and of course, authentication and authorisation.

New threats, risks, and vulnerabilities as well as evolving business requirements underscore to the need for a strong authentication approach based on simple service delivery, choice, and future-forward scalability.

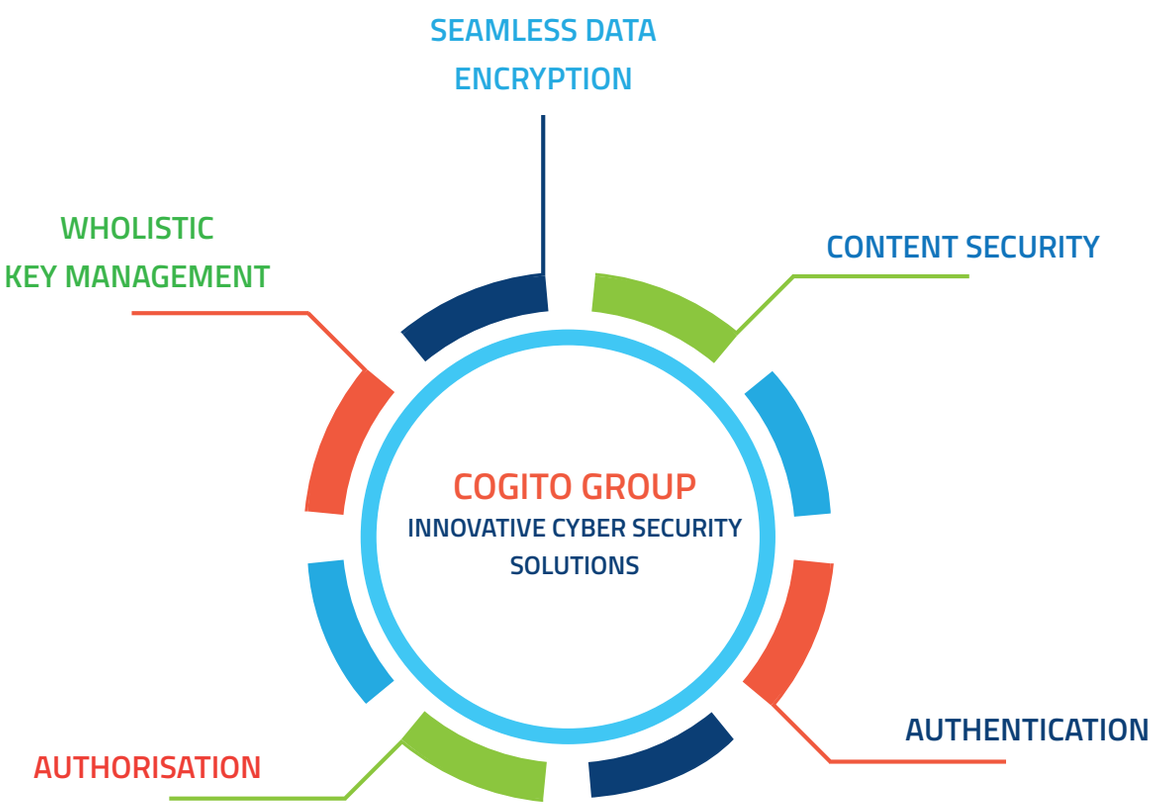
Today, organisations are asking:

- Can I address new demands of my business — like cloud and mobile devices?
- How do I map access control methods to business risk and the needs of my users?
- Can I centrally manage, control and administer all my users and endpoints?
- Who controls my user data?
- How can I incorporate additional security layers to help me further fortify against threats?
- And how do I keep it all practical and cost-effective?

More than ever, customers are looking for data encryption; identity and access management solutions; and identity and relationship management solutions that deliver simplicity, automation, reduced TCO and choice.

THE SOLUTION

Identity Management and Data Protection



Identity and Access Management (IdM and IdAM)

IdM is the management of individual and device identities, their authentication, authorisation, roles, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.

IdM is inextricably linked to the security and productivity of any organisation involved in electronic commerce.

ID management systems give organisations a way to control the swarm of untethered devices (Network Equipment, Computers, mobile devices) in the enterprise. An added benefit is departments, agencies and companies are using IdM systems not only to protect their digital assets, but also to enhance productivity.

Public Key Infrastructure (PKI)

A PKI is the basis for the providing of secure and trusted credentials. These credentials are used to establish trust in electronic transactions that the parties or systems involved are who they claim to be.

Cogito Group currently provides support, maintenance and enhancements to the largest PKI installation within Australia.

Security and Data Protection

Cogito Group security products provide key management and protection and Data encryption for:

- Databases
- Files and file systems
- Storage units
- Directories
- Applications

These security products provide protection of data in transit and at rest and are ideal for implementation in physical, virtual or cloud environments.

Hardware Security Products

Our Hardware security products include Hardware Security Modules (HSM's), Tokens, Smart Cards, Readers, Secure USB Keys, Secure SANs and Firewalls.

Our HSM's provide a high level of protection for transactions, identities, and applications by securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services. Performance is enhanced through a larger transactional throughput.

Our smart card, smart card reader, USB and OTP tokens respond to the needs for strong authentication, data loss prevention, compliance to governmental security directives and the growing demand for qualified digital signature.

Our firewall products allow more traditional boundary protection to be achieved, while our secure storage options allow for a greater level of data assurance and protection wherever that equipment may be located.

Protection in the Cloud

Cogito Group provides services for the protection of cloud solutions (internal, external and hybrid). These include:

- Virtual server protection and encryption
- File encryption
- Database encryption
- Secure Storage from the customer's site
- Secure Cryptographic Key Storage

Identity as a Service (IDaaS)

Cogito Groups IDaaS service offers identity and credential management, backed by an accredited PKI.

Card/Credential Management System

Card/Credential Management Systems are used to manage the association between an identity and their issued credentials. They manage the lifecycle of trusted tokens such as smart cards and now provide capabilities for the management of virtual smart cards and credentials delivered to smartphones and other mobile devices.

OUR EXPERIENCE

Key Capabilities

- **Delivered the largest and most geographically dispersed smartcard implementation in Australia for the ADF, issuing over 2 million soft and hard token certificates in its lifetime.**
- **Delivered the largest Public Key Infrastructure for the ADF. Provided the installation, integration and testing services to a new facility to allow the joining and access of other networks to the ADF's environment at the Highly Protected network level.**
- **As part of interoperability between ADF and its allies achieved PKI Interoperability agreements between US DoD and ADF high and low networks. Ensured future proofing of cross certification solution.**
- **Delivered the most advanced boundary defence and inspection services available anywhere in the world today by providing capability for use in high security environments.**

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 a 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, and 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).

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.

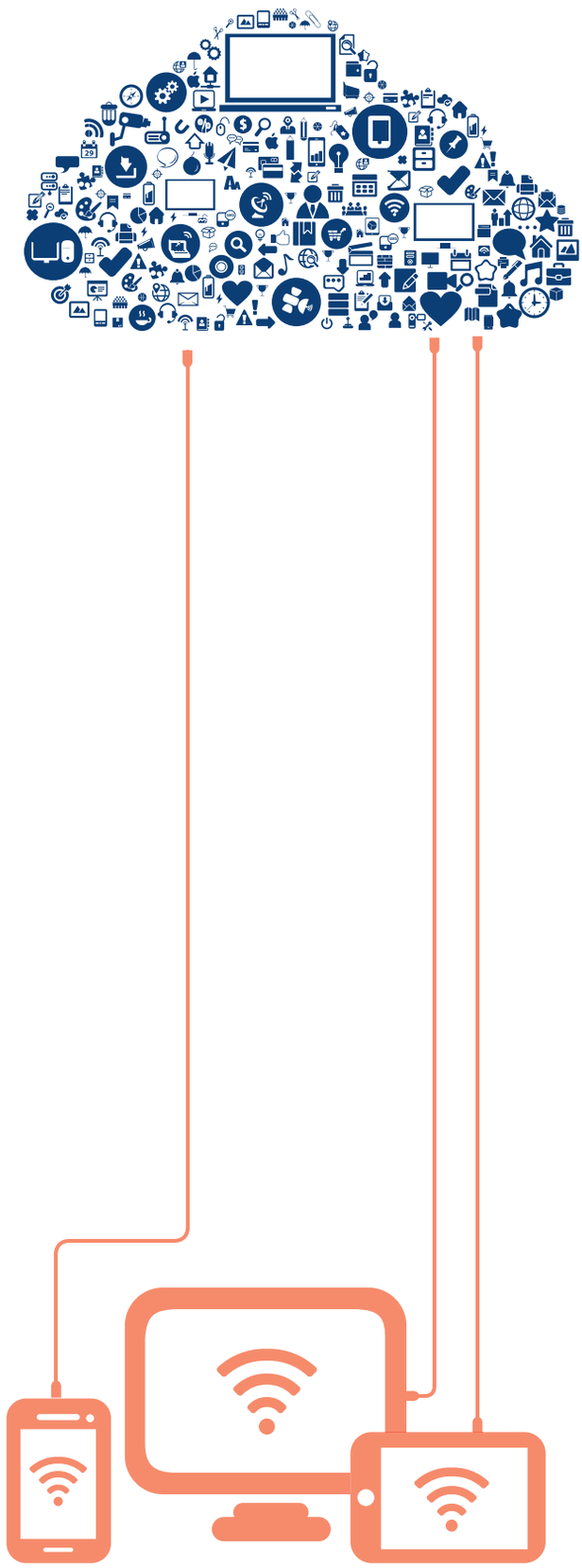
Security Architecture
Personnel Location Change Detection Service (PLCDS)

Cogito developed a service business workflow called Personnel Location Change Detection Service (PLCDS). This service was designed to identify a change in a person's location within the organisational structure and once identified, it will automatically deprovision a user from the service associated with their old role in order to save on licensing costs.

RO Terminals

As part of the work to join Australian trust points to trust points with other nations, Australian Defence required the rollout of Multifactor Authentication enablement for a specific user population. This required specialised terminals that were seen by the national partners to not have the same risks that were associated with the main networks (i.e. terminals for registration that were stand-alone).

Cogito developed the design that could meet a requirement to rollout Registration Officers (ROs) terminals around Australia. The solution allowed central management, update and maintenance of those terminals in the field.



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.

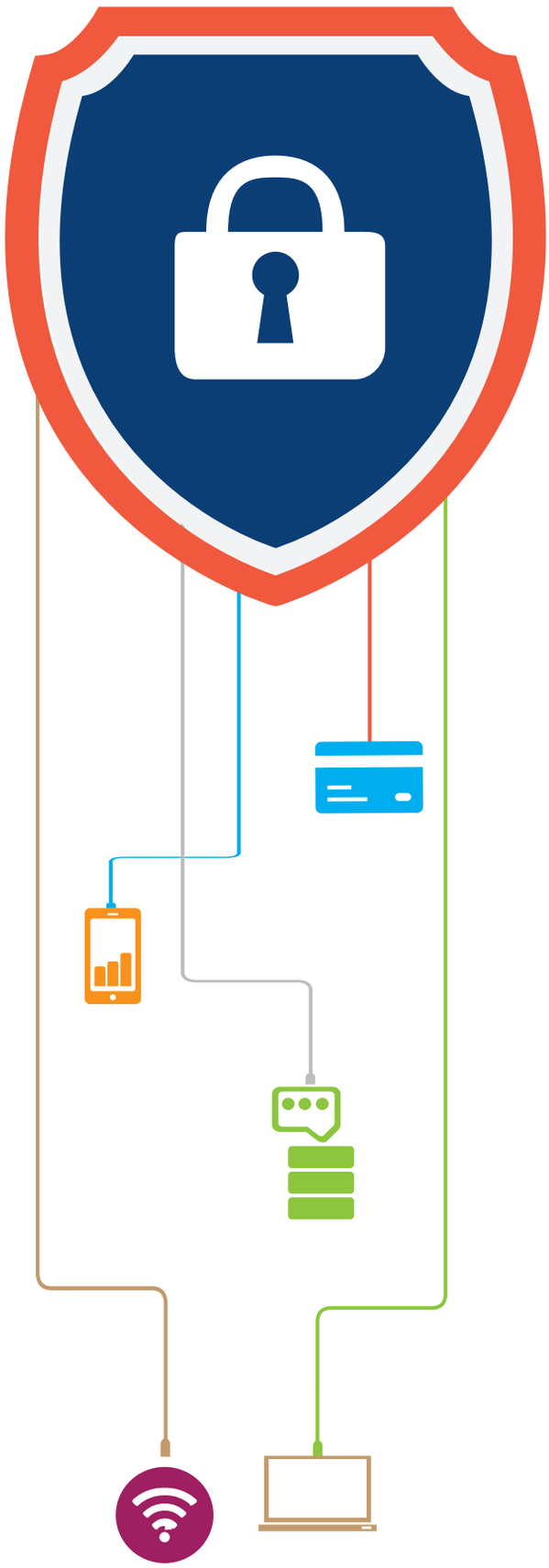
Integration Specialists

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.

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.



OUR PRODUCTS AND SERVICES

HARDWARE

Card Printers	Fargo Card Printers
Hardware Security Modules	SafeNet CA3, SA4, SA5, G5, Virtual HSMs
Network equipment	Palo Alto, Cisco, Alteon, F5BigIP, Brocade,Avaya
One Time Password Tokens (OTP)	SafeneteToken PASS OTP Authenticators, SafenetGOLD OTP Challenge Response Token Gemalto
Readers	ASK, Gemalto, SCM, Cherry, Omni
SmartCards	Oberthur PIV cards, Gemalto PIV cards, SafeNet SC650 cards and Datakey 330 cards
Storage	Netapp

CONSULTANCY

- Administrator (Network, Storage and Platform)
- Business Analyst
- Business Intelligence and Analytics
- Certification of Networks, Gateways, LANS and Security Operations
- Configuration and Change Management
- Data Modelling
- Directories specialist
- Integration Specialist
- IT Security Architecture
- IT Security Policy, standards and technical instructions
- Messaging specialist
- Project Manager
- Sustainment Services
- Systems Analyst
- System Engineers
- Tester
- Technical Specialist

SOFTWARE

AntiVirus Security	Bitdefender
Card/Credential Management Systems	Intercede: MyID CMS Versatile Security: vSec CMS Certified Security Solutions: Certificate Management System
Cloud Security	Safenet: Protect-V, ProtectFile, ProtectDB, Protect App, Cryto Command Center; Network Encryption Products
Data Encryption & Crypto Management	Safenet: ProtectApp; ProtectDB; Tokenization Manager; ProtectFile; ProtectV; SafeMonk; StorageSecure; KeySecure; KeySecure with Crypto Pack; Virtual Key Secure
Multi-Factor Authentication	SafeNet Authentication Manager SafeNet Authentication Manager Express (SAMx) SafeNet Authentication Service SafeNet Authentication Client GemaltoIDConfirm
Identity Management: IdM; IdAM; IdRM	Oracle Suite ForgeRock: OpenAM; OpenIDM; OpenDJ; OpenIG Evolveum: Midpoint

OUR SKILLS MATRIX

Cogito Group consultants have specialist knowledge in following: Applications | Languages | Standards and Protocols.

Administration

MS Word, Excel, Visio, Project

Card/Credential Management System (CMS)

Intercede MyID CMS, Versatile vSec CMS, Certificate Management System from Certified Security Solutions.

Cloud Security

Safenet Key Secure, Protect-V, ProtectFile, ProtectDB, Protect App, Tokenization Manager, StorageSecure.

Cloud service support and integration

AWS, Azure, Office 365 3rd party security integrations.

Database

SQL Server database technologies

Oracle RDBMS 9i/10g/11g/12c

MS SQL Svr 7/2000/2005/2008/2012/2014

Directories

Nexor

View500/View DS

Adam/AD LDS

ForgeRock OpenDJ

Various X.500/LDAP Directory Services

IDM/IAM/IRM

Oracle Identity Manager/Access Manager etc

Forgerock Open (AM, IdM)

Sun Identity and Access managers (superseded by above two products)

Evolveum MidPoint

Microsoft

Active Directory

MS Exchange

Microsoft Certificate Services

Microsoft OCS/Lync

MS OCSP

MS SharePoint

Monitoring for Systems and Networks

Nagios, Wireshark

Operating System

Microsoft Windows NT/2000/XP/Vista/7/8/8.1

Microsoft Windows NT/2000/2003/2003 R2/2008/2008 R2/2012/2012 R2 Unix; Solaris; Linux (various such as Ubuntu, RHEL, CentOS and Fedora)

Other Applications

SMTP Mail Administration

Lotus Notes/Domino

IIS

Isocor X.400 mail servers

ArcServe IT Backup software

Content Technology MimeSweeper

SAP NetWeaver DSE

Axway Validation Authority

MobileIron

Physical Access Control

Gallagher PIV PACS

Public Key Infrastructure (PKI)

UniCERT, Entrust, MS CS, Redhat CS, Fedora Dogtag, EJBCA, OpenSSL

Smartcard and OTP Middleware

Safenet High Assurance Client, Safenet Authentication Client, Safenet Authentication Manager

Charismatics CSSI

Web Support

Apache, Apache Tomcat, Apache proxy, IIS

Virtualisation

VMware vSphere, vCentre

Microsoft Hyper-V, SCVMM

Zen

PROGRAMMING LANGUAGES

- Android development
- ASP
- Bash Scripting
- C
- C#
- C#.NET
- C++
- HTML
- Java
- JavaScript
- .Net
- Perl
- PHP
- PowerShell
- Python
- Ruby
- SQL/PL SQL
- VB.Net
- VB Script
- Windows batch scripting
- XML

STANDARDS AND PROTOCOLS

- Allied Communications Publications 133, 123, 128
- Department of Finance, Gatekeeper (GK) Accreditation
- Department of Finance, 3rd Party Identity Services Assurance
- FIPS – 140, 201
- NIST SP 800 – 90b, 73, 53, 131
- ISO 27001 – Information Security Management
- LDAP
- Public Key Cryptography Standards (PKCS)

Security

- Australian Government Information Security Manual (ISM)
- Protective Security Policy Framework (PSPF) X.500 Directories standards X.509 PKI

Request For Comments (RFC)

- RFC 3820 – Proxy Certificate Profile
- RFC 5246 – Transport Layer Security Protocol
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and
- Certificate Practices Framework
- RFC 5280, 6818 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 4510 (and associated LDAP RFCs) – Lightweight Directory Access Protocol (LDAP)
- Draft-nourse-scep-23 – Simple Certificate Enrolment Protocol
- RFC 2560, 6960 – Online Certificate Status Protocol (OCSP)

ABOUT COGITO GROUP

Cogito Group is an Australian owned and operated ICT Company. We are digital security experts and specialise in 'enabling technology' that keeps your physical, logical and cloud based data and infrastructure safe. Examples are Identity and Access Management systems, one time password tokens, smart cards, card management systems and public key infrastructure.

Cogito Group will protect your information: where ever it sits and however it is received.

Cogito Group are designers, system integrators and sustainment specialists. We 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 solutions are designed to integrate multiple products and technologies to achieve your digital security goals.

Cogito Group

OIX OPEN IDENTITY EXCHANGE

fido alliance member

kantara INITIATIVE

AUSTRALIAN BUSINESS AWARDS 2014 FINALIST

Phone: +61 26140 4494 Email: sales@cogitogroup.com.au www.cogitogroup.com.au