Fact Sheet

Cogito Group

Public Key Infrastructure as a Service

Who Are We?

Cogito Group – Specialist Providers of Authentication Solutions

Established in 2011, Cogito Group is an ICT company that specialise in Public Key Infrastructure (PKI), Identity Management (IdM) and data protection using next gen authentication encryption 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.

We are designers, system integrators, and sustainment specialists. We specialise in bringing together component subsystems to create holistic organisational security postures. Our focus is bridging the common operational gaps faced in the integration of digital security technology. Our solutions are designed to future proof your organisation against the ever-changing cyber threat landscape. We protect your information wherever it sits and however it is received.

Professional Services

Cogito Group consultants provide specialist advice to clients regarding digital security solutions. We focus on operational efficiency, risk mitigation, vulnerability analysis, regulatory compliance, audit and reporting for digital security systems. Our Professional Service offering includes:

- Design, build, and sustainment of Public Key Infrastructure.
- Assistance, advice, and management of Public Key Enablement (PKE) such as securing and managing enterprise devices and capability as well as Bring Your Own Device (BYOD).
- Solution Accreditation and Compliance for digital security systems.
- Deployment and use of digital certificates.
- Deployment and use of Hard Token technologies such as Smart Cards.
- Security Policy and Security Quality Management.

Ongoing Support

Cogito provides ongoing support, maintenance, and implementation/upgrade services. We keep our clients aware of new technology to ensure their systems maintain peak performance and optional levels of security. We do not provide a static solution; our products are purpose built to handle complexity and designed to evolve with ever changing security requirements.

PKIaaS White Paper

Fact Sheet

What Do We Do?

Public Key Infrastructure

Public Key Infrastructure (PKI) is a system of cryptographic technologies, standards, management processes, and controls governing the use of digital certificates. It is an enabling technology. This means it enables users of an insecure public network (such as the internet) to securely and privately exchange data through the use of a public/private cryptographic key pair that is obtained and shared through a trusted authority.

NIST SP800-32 defines PKI as "binding public keys to entities, enabling other entities to verify public key bindings, and provides the services needed for ongoing management of keys in a distributed system".

The Business Need: Enabling Trust

Cogito Group provides high assurance cyber security solutions, such as Public Key Infrastructure, that are necessary to establish a hierarchal chain of trust to certify users and devices.

Cogito Group can meet your business needs and ensure solutions offered meet the evolving security needs of the organisation by taking into account:

- The volume of certificates issued by the CA.
- The number of applications to be supported.
- Compliance & auditing requirements.
- Evolving requirements of the agency.
- Geography and topology.
- Existing cryptographic policies and legacy systems.

The Challenge: Complexity and Inexperience

Organisations that don't specialise in PKI solutions are often challenged and do not have the necessary skills to establish a trustworthy and resilient PKI, particularly that can take into account complicated factors such as mobility, cloud computing, and Internet connected devices bring.

Cogito Group can meet these complex challenges. We specialise in this niche area and have skilled, security cleared citizens to provide these services.

The Solution

We provide our clients with on-premises and as a Service PKI solutions that can support small or large numbers of users, devices, software applications, business systems, and organisations across simple or complex ecosystems. We provide our clients with solutions that ensure data remains in-country and services are provided by security-cleared citizens.

The Benefits

The benefits of a PKI are numerous as it provides a foundation for confidentiality, data integrity, authentication, and non-repudiation. It's what we call enabling technology. PKI use cases include:

- Wi-Fi Authentication – multi-tenanted government office accommodation environments.

- Voice and Video Conferencing – GNet secure voice and video transport (DTLS/SRTP).
- User Authentication – especially where high assurance and non-repudiation is required. Protocols such as SAML, OATH, and others based on X.509 certificates can be used for Single Sign-On (SSO) over GNet and mutual authentication of both users and devices.
- End User Device / Organisational / Hardware Authentication.
- Line of Business System/Application Authentication and Verification.
- Signature Verification – for agency systems, online forms signing for users.
- PKI Managed Service – Use of the TaaS Catalogue construct allows most agency-managed PKI environments and system requirements to be met through a 'PKI as a Service' like catalogue of selectable services.
- Communities of Interest (CoI) – Enabling creation of CoIs by adding registered endpoints to a group using a shared key, which means CoIs can be created very quickly and cheaply on an ad-hoc basis. GNet is an example of a permanent, large scale, CoI.

What Are Our Services?

PKI Services - New Zealand All of Government PKI as a Service

Cogito Group were selected by the Department of Internal Affairs (DIA) to run their All of Government (AoG) Root CA and the GNet policy CA for the New Zealand Government. This solution assists New Zealand government agencies improve security by guaranteeing high assurance on critical systems.

The New Zealand Government Public Key Infrastructure Framework (PKIF) governs the use of digital certificates and cryptographic keys issued through the New Zealand Government Public Key Infrastructure (PKI) to assure the identity of affiliated entities. These entities may include persons, devices, software applications, business systems and organisations acting for or on behalf of the New Zealand (NZ) Government

To provide this service, it was critical data remained in country and services were provided by security cleared citizens. Cogito Group also built the backend product, Jellyfish to support the service. This TaaS as a service model allows us to deliver constant innovation to our clients as we can adopt to new technologies faster, with no waiting for an upgrade cycle. It lowers the configuration and change management burden on organisations and importantly does not lock them into a vendor.

Cogito Group has several offerings for the delivery of PKI services to subscribing agencies. These solutions range from the provision of management services for existing PKI implementations, implementation and management of new on-premises PKI services and the provision of PKI as a Service.

PKI Management Services

Cogito Group can provide personnel for the management of the day to day operations of existing PKI systems. This includes management, solution support and enhancement. Cogito Group has significant expertise in providing these services and currently provides support to one of the largest,

complex PKI implementations in the southern hemisphere with the Australian Department of Defence.

PKI Implementation and Support

Cogito Group are able to provide personnel for the implementation and ongoing support of PKI services. These services include the following:

- Solution architecture and design.
- Project management.
- Solution implementation.
- Provision of specialty hardware including Hardware Security Modules, Credential Management Systems, and Smartcards.
- PKI management services.

Cogito Group has extensive knowledge of the design, implementation, and support of PKI systems. Cogito Group has developed this knowledge through being involved in the design and implementation of one of the largest and complex PKI implementations in the southern hemisphere with the Australian Department of Defence. This knowledge includes the design and implementation of the existing PKI service, and the cross certification of the PKI solution with other agencies.

PKI as a Service

Cogito Group's PKI as a Service provides a hosted fully managed PKI service, available to agencies to consume without the associated setup cost of an on-premises solution. The service provided will allow agencies to select the level of security and assurance they require for the establishment of trusted identities and services within their organisation.

Services offered from the Cogito Group PKI as a Service include:

- Credential Management.
- Identity Registration.
- Local or hosted credential printing.
- Shared or dedicated CAs.
- Shared or dedicated Hardware Security Modules.
- Shared or dedicated infrastructure.

What is Included in the PKI as a Service?

Cogito Group includes in the offering:

- 2 CRL publication points and OCSP (for the shared CA option).
- Hardware key protection of the CA.
- Full self-managed portal - users submit and revoke requests.
- Notifications:
  - Users alerted when manually created certificates are going to expire.
  - Extension to managers (or others) if that user does not respond or has left the organisation.
- Portal provides reporting on usage and billing.
- View untrusted certificates.
- Replace multiple CAs.
- Replace external SSL certificate provider.
- Optional automatic enrolment capability:
  - Multiple Windows domains from the one CA.
  - Automatically enrol Linux.
  - External certificate support (through a Let's Encrypt option).
  - Automatically enrol SCEP services such as network switches and routers.

Best of Breed Security

We ensure a solid foundation. This includes:

- A no lone zone for production systems.
- Security cleared citizens (the standard clearance level for our staff is now at Top Secret).
- Special safeguards on the storage of the equipment.
- GCSB inspected hardware for Government service.
- Accredited data centres with independent physical/logical security controls.

Cogito Group is involved in the largest and most complex PKI implementations in the Southern Hemisphere with our client the Australian Department of Defence.

PKIaaS White Paper

Fact Sheet

Cogito Group is the only operational provider of PKIaaS in NZ that has Government certification and we are the only known provider that has achieved NZ Government certification with no requirement for any remedial actions. No other provider has an operational aaS solution in New Zealand.

We only provide dedicated services:

- All PKI/IdM security services sit in their own dual firewalled off enclaved environment.
- No shared resources such as web servers.
- Each organisation is separately tenanted giving full separation between each service.
- Customer dedicated CAs are separated from other customer CAs.
- Lateral security components (i.e. even if a trusted insider were to find a way to compromise the CA network, they still can't cross from their components to the components used by another customer).
- Zero Trust.

We have a number of certifications such as ISO 27001 which dictates the international standard regarding the management of information security. Bulk revocation comes with safeguards to prevent a denial of service attack by trusted insiders.

Full Management Interface and Self-Service

Modular solution offers choices. If you only require Auto Enrolment:

- Take control of your issuance and revocation.
- Delegate that authority to those you deem fit to give it to.
- Pay no more than you do for an automatically enrolled certificate.
- With sufficient rights, you can request a new CA in the interface although this does require some interaction with a customer to complete. You can also use your internal service management tools, such as ServiceNow and BMC Remedy, rather than our portal.

If your organisation may want more than auto-enrolment:

- Full manual issuance interface allows provisioning of other services within your environment should you allow it, not just the provisioning of certs.
- Receive alerts on untrusted and trusted certs.
- Full reporting - You can create your own custom reports around usage of our services.
- Full intelligent search - You can do all sorts of searches in our interface (Examples include subject line; expiry; certificate key usage; Key Encipherment; namespace).
- IdM backed services reporting to ensure expiring issued manual certs are replaced.
- Full CMDB for device, user, application and service centric management.
- Full provisioning and de-provisioning tasks you'd expect from an IdM as well as Single Sign On, and dynamic access management. All through the one integrated interface.
- One stop interface for a number of security services. Our products were made to service enterprise and small customers alike. That means our solution includes other features like integrated monitoring, SIEM, Anti-Virus, Identity and Access Management, Id Brokerage, Single Sign On, Physical Access Control System integration, secure dropbox like services etc.

- Inbuilt service management capability. If you can't do something in the interface that you need to do, you can submit a service ticket right there without leaving the interface.
- Full key management capabilities including Hold Your Own Key (HYOK) and Bring Your Own Key (BYOK) options for services such as Azure and AWS.

What Are the Products?

Pricing is dependent on the services consumed and outlined in the TaaS Price Book via the DIA TaaS Portal. We recommend options based on needs and size of the organisation. Some examples are outlined below.

Option 1: Price Per Cert Manual Issuance Using Portal

Price Per Cert Manual Issuance Using Portal	
PD 4.1	Setup cost - $197.37 per hour in 8-hour blocks.
PD 4.7	Certificate Template under management - $100.00 per month per template in use.
PD 4.8	Certificate Issuance - Auto Enrol Soft Certificate or manual certificate issued by client Registration Officer - $150.00 per certificate per year.

Ongoing cost of per month for these organisations based on 50 certs is $8,700.00 per year. This may be higher if more certs were required or a change of certificates were to occur. This option has no automated assistance, with everything manually issued by internal staff.

This is recommended for environments that do not intend to issue more than 50 certificates as when managing more than 50 certificates, this option becomes more expensive than other options and provides no automation. Actions must be completed manually once a year or whenever a device or service is rebuilt/replaced. The service, however, does provide notifications allows you to search for expiring certificates.

Option 2: Per Cert Automatic and Manual Issuance Using Portal

Price Per Cert Automatic and Manual Issuance Using Portal	
PD 4.1	Setup cost - $197.37 per hour in 8-hour blocks.
PD 4.5 PD 4.6	Auto Enrolment (AE) Service Server - $400.00 per month per AE service.
PD 4.7	Certificate template under management - $100.00 per month per template in use.
PD 4.8	Certificate Issuance - Auto enrol soft certificate or manual certificate issued by client Registration Officer - $150.00 per certificate per year.

Ongoing cost of per month based on 50 certs is $14,700.00 per year. This may be higher if a second certificate were required or a change of certificates were to occur. This is a good option for under 50 certificates as it is the lowest cost with full automation for the low certificate count. Manual certificates can still be issued as required.

Option 3: Per Cert Automatic Per 100 Certs

Price Per Cert Per 100 Certs	
PD 4.1	Setup cost - $197.37 per hour in 8-hour blocks.
PD 4.5	Autoenrollment (AE) Service Server - $400.00 per month per AE service.
PD 4.7	Certificate template under management - $100.00 per month per template in use.
PD 4.11	Certificate bundle of 100 automatically issued certificates - requires AE service – $2,196.00 per month.

Ongoing cost of per month for these organisations based on 100 certs is $2,696.00 per month or $32,352.00 per year. This includes extra certs in case of a second cert being required or a change of certificates were to occur. This option additionally has an automated facility.

Option 4: Per User NOT Per Cert Option. Up To 250 Users And 500 Active Certs

Price Per User. Up To 250 Users And 500 Active Certs	
PD 4.1	Setup cost - $197.37 per hour in 8-hour blocks.
PD 4.5	Autoenrollment (AE) Service Server - $400.00 per month per AE service.
PD 4.7	Certificate template under management - $100.00 per month per template in use.
PD 4.12	Small organisation user certificate bundle - Per user based on AE issued certificates. Small user base (this would be useful for a pilot of the capability). This option does require AE. All changes require PS. Maximum of 500 certificates under management. - $1,385.00 per month.

Ongoing cost of $1,885.00 per month or $22,600.00 per year. This option gives greater flexibility to the organisation and they can issue more than one cert per user/device. Only valid certificates (i.e. not expired or revoked certificates count in the per month amount allowing the organisation to reissue as often as they want without further charge.). This option is only for smaller organisations with 250 or fewer users.

Option 5: Shared Issuing CA

Shared Issuing CA	
PD 4.1	Setup cost - $197.37 per hour in 8-hour blocks.
PD 4.2	Shared Issuing CA ongoing cost - $5,261.67 per month.
PD 4.5	Autoenrollment (AE) Service Server - $400.00 per month per AE service.
PD 4.7	Certificate template under management - $100.00 per month per template in use.
PD 4.20	Certificate Issuance - Auto enrol soft certificate or manual certificate issued by client Registration Officer $5.

Ongoing cost of per month for these organisations based on 100 certs is $5,761.67 per month + $500 a month for certificates. That is a total of $6,261.67 a month or $75,140.04 per year. This, however, is not a dedicated service and would be shared with other customers of Cogito Group.

This can dilute the trust you can place in the CA but is effectively what all the public trust CAs do. Recommended only for small organisations that are willing to accept the trust risks.

Option 6: Dedicated Issuing CA

Dedicated Issuing CA	
PD 3.1	Setup cost - $197.37 per hour in 8-hour blocks.
PD 3.4	Issuing CA ongoing cost (includes 500 certificates) - $10,170.00.
PD 3.8	Certificate Issuance - Auto enrol soft certificate (500 included in setup) – 0.18c per cert per month past the first 500.

Ongoing cost of per month for your organisation based on less than 5000 certificates under management is $10,170.00 per month or $122,040.00 per year for the longer-term enterprise approach.

Optional Components

In addition to the components above, some of the more common optional components are listed below. They are:

Optional Components	
PD 3.7 PD 4.5 PD 4.6	Windows Autoenrollment (AE) Service Server - $400.00 per month per AE past the first one. You get one included so the cost of this is usually $0.
PD 3.20	Managed CA as a Service - Validation Authority Software (Management) - $1,731.00 per month. You can do without this as well if you don't want external validation. You just set one up internally (say on the AEP and another server) and go from there.
PD 3.37	Certificate template under management - $100.00 per month. Cost should be $0 as two templates are included.
PD 4.21	SSL/TLS Intercept Certificate with active management - $2,154.00 per cert per year
PD 4.23	External certificate with public trust with 1 SAN included - $300 USD per cert per year.

Under Management

Under management means that if you revoke certs they are still searchable but don't count for billing purposes anymore (i.e. no monthly charge). This solution would be a dedicated service and give you a level of autonomy from other organisations.

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.