

Hardware Security Modules

Best of Breed

Cogito Group offer the best of breed identity management and digital security hardware and software products. We partner with leading international hardware providers to ensure we deliver product solutions that are tailored to the needs of our clients. Our Hardware security products include Hardware Security Modules (HSMs), Tokens, Smart Cards, Readers, Secure USB Keys Secure SANs and Firewalls.

Our HSMs 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. HSMs are specifically designed to be resistant to both physical and logical attacks, and to not leak sensitive information, as described in the FIPS Security Policy.

HSM Deployment Services

Cogito Group deploys HSM units in production environments. Deployment consists of the following high-level tasks:

- Onsite HSM deployment with installation of features, licenses, and configuration in the production environment.
- Provision of as-built documentation.
- Initial key ceremony.
- HSM support.
- Integration to monitoring and logging (SIEM) systems.
- Implementation of management features including remote administration.
- Provision of Key ceremony documents.
- Operator training.
- Installation completion and acceptance into production.

HSM Security Controls

HSMs controls access to keys through both Access Control Lists (ACL) and Operator Cards. Any key generated by the HSM has its own key ACL controlling how that key can and should be stored, how its use is authorised, and whether that key can be wrapped for external transport. Keys cannot be exported in cleartext. The key's ACL binds its use to a particular function. For example, a private key can be generated that will only allow signature operation and not decryption.

All cryptographic operations that relate to use of HSM protected key material take place within the security area of the HSM. These transactions are not visible to any external processes. Invalid command sequences will be rejected and will not affect functionality.

Sensitive material residing in the HSM is cleared when it is no longer needed by a calling application. As a further protection, if the HSM goes into an error state it will immediately stop accepting any connections and must be rebooted in order to recover. HSMs support SNMPv3 monitoring which can be used to alert on HSM health and status.

Auditing is enabled when you generate a key. When turned on, every function involving that key will be audited. Authentication to the HSM is via a password or a 'M of N' smartcard set allowing enforcement of multiparty two-factor authentication. This means you can enforce multi-person operation or for mandatory "no-lone zones". The protection of keys is defined at the time of creation, allowing for different authentication requirements for use of different keys.

Cogito resells HSMs that are accredited to FIPS140-2 Level 3. As such, our HSMs contain a tamper-proof area in which the HSM device resides. Any attempt to access this tamper-proof area results in a factory reset of the HSM being triggered. This erases any key material present in the HSM. If someone were to get inside the tamper-proof area, there is further tamper-proofing within the HSM card itself at the FIPS boundary. Any attempt to access this zone destroys the HSM.

The user serviceable zone contains the power supplies and fan tray. No access is available to the tamper-proof zone through the user serviceable zone. The components within the user serviceable zone are replaceable and commercially available.

HSM Use Cases

Cogito Group have an extensive history in HSM integration work in New Zealand, Australia, and internationally. HSM's can be integrated with all applications and protocols listed in the requirement, and additionally, may also be integrated for the following use cases:

- AWS Bring Your Own Key (BYOK).
- Azure BYOK.
- Certificate Authorities.
- Primekey EJBCA.
- Active Directory Certificate Services.
- Unicert.
- Entrust.
- Microsoft Authenticode Signing.
- Database encryption.
- MySQL / MariaDB.
- PostgreSQL.
- TLS offload for Load Balancers and Web Services.
- TLS intercept/Data loss prevention.
- eMRTD Document Security Object Signing.
- eMRTD Active Authentication Key Generation.
- Password and Secret Management.

Cogito Group have extensive experience in writing Security Policy and operational documentation including Cryptographic Key Management Plans, Certificate Practice Statements, and Key Ceremony documentation, and will ensure that the solution is fully compliant with sovereign security requirements. Cogito Group offer cryptography and security expertise, with trained and professional resourcing available.

Case Studies

Air Services Australia

Cogito Group implemented HSM products and Remote Administration capability for Air Services Australia. The HSMs were delivered to the client in original packaging, complete with tamper seals and declaration of Country of Origin. Cogito Group provided a seal checklist and witness forms to provide accountability and auditability of the event. An initial Key Ceremony was performed with Air Services staff to generate the Administrator Card Set (ACS) and Operator Card Set (OCS) as part of the creation of the Security World. Cogito Group provided Key Generation Ceremony scripts and documentation to support this process. Cogito Group also enabled additional feature sets for the HSMs.

Cogito Group configured network connectivity to the HSMs and set up the Remote Management, RFS, Configuration Auto-Push, and High Availability features. Monitoring and logging for the HSMs was also configured as part of this process. Cogito Group provided full as-built documentation for each of these tasks.

CyberArk was also configured to use the HSMs, and a second Key Generation Ceremony was performed to generate the CyberArk encryption keys. Ceremony documentation was also provided by Cogito Group.

Australian Defence Organisation

Cogito designed, supplied, installed, configured, and maintain ADO's HSM fleet, which is the largest HSM fleet in Australia. These are used primary for PKI services.

Cogito Group has managed the HSM's for Australia Defence CDMC team since 2014. This has involved delivering the upgrade of all Hardware Security Modules (HSMs) within CDMC of Defence. This involved upgrading of all client/management software that utilised these devices in addition to the physical device replacement. Cogito Group delivered a comprehensive test plan, involving testing of functional requirements, non-functional requirements, high-availability mechanisms, and backup/restoration processes.

Over this period, Cogito Group has worked on several projects within CDMC including the SHA1 and SHA2 infrastructure complete with HSM upgrades, SIPR Connectivity, and SIPR REL A projects for the implementation of HSMs in support of the F5 and OCSP services.

Australian Taxation Office

Cogito is responsible for assisting ATO in configuring the HSMs that support their MyGov PKI. This includes instructing on use of the PED and how to partition HSMs. Cogito Group trained ATO staff, developed accreditation document and co-ordinated and ran the Key Signing Ceremonies. Cogito Group was also responsible for ensuring stronger security controls were put in place at ATO.

New Zealand Government Clients

Cogito Group utilises HSMs in our own Authentication as a Service operation within New Zealand. Our New Zealand operations is largest deployment of HSMs in the country that we are aware of. They are used for a number of key management tasks including internal and customer PKI services.

Cogito currently maintain the HSM's and cryptographic management for over ten New Zealand Government Agencies. Some examples include:

- Cogito Group was selected to run the New Zealand Government All of Government PKI in order to assist agencies in improving security by guaranteeing high assurance on critical systems.
- Cogito Group manages the security behind New Zealand ePassports issuing all certificates and keys used in New Zealand ePassports. The ePassport validation process determines the authenticity and integrity of an ePassport as well.
- Cogito Group have addressed many of the New Zealand Internal Revenue Department's security challenges caused by various mobile, cloud computing, and internet-connected devices, through deploying Authentication as a Service solutions. Cogito group have also helped Inland Revenue in securing their cloud services by protecting and managing the encryption keys associated with such services.
- Within the New Zealand Defence Force, Cogito Group have designed the authentication services that have been deployed to their tactical and strategic environments. This will enable a major and fundamental step forward in securing data internally to their network, as well as allow for more secure communications with their national and international partners.

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.