HSM Specialists

High level protection for transactions, identities and applications

Securing cryptographic keys. Provisioning encryption, decryption, authentication and digital signing services.

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.

The HSM is specifically designed to be resistant to both physical and logical attacks. The HSM is designed not leak sensitive information, as described in the FIPS Security Policy

HSM Deployment Services

Cogito Group will deploy the HSM units in production environments. Deployment consists of the following high-level task:

- 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

Cogito Group
www.cogitogroup.net

HSM Security Controls

HSMs controls access to keys through both an Access Control List (ACL), and Operator Cards. Any key generated by the HSM has its own key access control list (ACL) controlling whether and how that key can 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 that key. When turned on, every function involving that key will be audited.

Authentication to the HSM is via either password, or a M of N smartcard set allowing enforcement of multiparty two factor authentication. This means you can enforcement more than one-person operation or for the enforcement of "no-lone zones" for instance. 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, 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 a further tamper proof zone 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 of the 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 Bring Your Own Key (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, and will ensure that the solution is fully compliant with sovereign security requirements.

Cogito Group are experts in creation of Cryptographic Key Management Plans, Certificate Practice Statements, and Key Ceremony documentation.

Cogito Group offer cryptography and security expertise, with trained and professional resourcing available.

Developing strategy that maintains integrity.

Case Studies

Air Services Australia

Cogito Group implemented HSM products and Remote Administration capability. The HSMs were delivered to Air Services 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 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.

Achieving Interoperability - joining Australian trust points to trust points with other nations.

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.

A number of projects Cogito has worked on within CDMC over this period include 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 was also responsible for ensuring stronger controls were put in place at ATO.

New Zealand Government Clients

Cogito utilise HSMs in our own Authentication as a Service operation in 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 NZ Government Agencies. Some examples include:

- Cogito Group was selected to run their All of Government PKI in order to assist NZ government agencies improve 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 security challenges faced by The New Zealand Internal Revenue Department that mobile, cloud computing and internet connect devices bring by 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 that are used to protect those services.
- Within NZDF Cogito Group have designed the authentication services that they will be deploying to their tactical and strategic environments. This will enable major and fundamental step forward in securing their data internally to their network as well as allow for more secure communications with their national and international partners.

Cogito Group is an award-winning 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
www.cogitogroup.net