Duty Location: **Mons, BEL**

JOB DESCRIPTION

Principal Technician (IdM and PKI Services)

NATO Cyber Security Centre

Grade: **G12**

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCI Agency delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

The NATO Cyber Security Centre (NCSC) is responsible for planning and executing all lifecycle management activities for cyber security. In executing this responsibility, NCSC provides specialist cyber security-related services covering the spectrum of scientific, technical, acquisition, operations, maintenance, and sustainment support, throughout the lifecycle of NATO Communications and Information Systems (CIS). The NCSC enables secure conduct of the Alliance's operations and business in the context of NATO's C4ISR. The NCSC provides cyber security services to NCI Agency customers and users, as well as to all other elements of the Agency; this includes all Service Lines, Programme Offices, CIS Support Units/Elements, and the Agency Ops Centre. The NCSC is responsible for providing the bread spectrum of services in the following specialist security areas: CIS Security, Cyber Defence, Information Assurance, Computer Security and Communications Security. In executing its responsibilities, the NCSC provides support to the development and implementation of cyber security-related policy, strategy, and provides lifecycle security risk management services for all NATO CIS. The NCSC leads in the development of new capabilities and innovation in cyber security. The NCSC incorporates and provides specialist services to prevent, detect, respond to and recover from cyber security incidents.

The Infrastructure Branch delivers a suite of enabling services in the specific areas of Cryptography, Identity Management, Technical Services (supporting CS Operations) and CIS Protection. These services include capability and validation of NATOs crypto solutions, lifecycle management of cryptographic equipment and keys, operation and logistic support for NATO-wide online and offline cryptographic equipment, identity management services, gateway services, specialized enterprise-wide CS infrastructure (including NCIRC elements), application, configuration and management of NATO Enterprise-wide endpoint security software.

The Crypto Services Section ensures lifecycle management of cryptographic equipment, keys provision for high grade Crypto, operation and logistic support for NATO-wide online and offline cryptographic equipment, Cryptographic implementation and site surveys. The section is also responsible for Crypto Compliance includes Crypto Facility/Maintenance Inspections and Crypto installations validation. The Identity Management/PKI Services Section provides Certificate Authority, Revocation and Lifecycle Management of digital certificates/entities and the appropriate training of registration authority personnel.

The IdM and PKI Services Cell is responsible for NATO Public Key Infrastructure (NPKI), which is a set of roles, policies, hardware, software and procedures managing the lifecycle of medium assurance asymmetric credentials. The NATO Public Key Infrastructure implements key management system capable of supporting a wide variety of Authentication, Integrity, Non-repudiation and Confidentiality services for the NATO Alliance.

Duties:

Under the direction of the Cell Head, the incumbent will perform duties such as the following:

- The planning and management of:
  - NATO wide Registration Authorities;
  - Control the lifecycle of end users for the NPKI;
  - PKI system backups and restore;
  - PKI virtualize infrastructure;
  - PKI networking components;
  - Keeping record of PKI hardware infrastructure;
  - Regular NPKI system components, firmware and Operating Systems (e.g. Red Hat, Windows) updates.
- Responsible for the NCIA ITSM ticketing system, provide regular updates and daily activity report;
- Responsible for Card Management System day-to-day management, support Smart Card enrolment process and provide troubleshooting;
- Responsible for certificates auto enrollment service; Entrust Admin Services interfaces;
- Install, configure and maintain the NATO Public Key Infrastructure (NPKI) systems and components;
- Install, configure and maintain the Hardware Security Module (HSM);
- Responsible for PKI system backups, restore and regular upgrade;
- Responsible for LDAP directory service, http and OCSP configuration and maintenance;
- Responsible for the operation of cryptographic security for all types of NATO funded PKI systems and associated equipment to meet Infrastructure Communications Project requirements;
- Supervises the day-to-day operations /management /backup of the PKI systems;
- Responsible for the creation of PKI related guidance;
- Provide technical support and assistance to NATO CIS Operating Authorities;
- Responsible for supporting all NATO exercises;
- Performs other duties as may be required;
- Deputise for higher-grade staff, if required.

Essential Experience and Education:

- Higher Secondary education and completed higher vocational training leading to a formal technical or professional certification with 3 years function related experience. Or a Secondary education and completed advanced vocational training leading to a professional qualification or professional accreditation with 5 years post related experience;
- Extensive knowledge of modern communication and Internet Protocol (IP) based networking technologies and systems including security aspects;
- 3 years extensive experience with PKI System installation and management;
- Extensive experience with 1st level user support;
- Extensive knowledge of Information security and Cryptography (symmetric and asymmetric encryption, public key infrastructure (PKI) encryption, public key encryption, hash functions, digital signatures, digital certificates);
- Must be familiar or proficient with NATO/National PKI security policies and procedures;
- Practical experience in Windows, Linux and VMware system administration;
- Knowledge of the principles of computer and communications security, networking, and vulnerabilities of modern operating systems and applications;
- Experience with SQL database administration;
- Extensive experience in operating systems backup and restore;
- Practical experience in scripting (Python, Powershell);
- Practical experience in SSL, TLS, and OpenSSL.

Desirable Experience and Education:

- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT;
- VMware (VCA, VCP) and Linux RHEL system administration certificates;
- Microsoft Certified Solution Associate (MCSA);
- Microsoft Certified Solutions Expert (MCSE);
- Experience in development and implementation of computer security policies;
- ITIL Concepts and Operation.

Language Proficiency:

- A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.
- **NOTE:** Most of the work of the NCI Agency is conducted in the English language.

Competencies or Personal Attributes:

- Achieving Personal Work Goals and Objectives - Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.
- Delivering Results and Meeting Customer Expectations - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.
- Adhering to Principles and Values - Upholds ethics and values; demonstrates integrity; promotes and defends equal opportunities, builds diverse teams; encourages organisational and individual responsibility towards the community and the environment.
- Relating and Networking - Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others.