Encryption / Key Management Support Specialist

NICE Framework Reference	None.	
Functional Description	Provides ongoing support to management and maintenance of virtual private networks, encryption, public key infrastructure, and, in some cases, Communications Security (COMSEC) in support of organizational IT security.	
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a significant impact on organizational IT systems, capabilities or functions.	
Development pathway	This is an often an entry-level job to the security domain after gained experience with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.	
Other titles	▪ Access management analyst ▪ System analyst ▪ Identity, credentials and access management (ICAM) specialist	
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians 2282 User support technicians	
Tasks	▪ Identify client requirements and propose technical solutions ▪ Install, configure, operate, maintain and monitor related applications ▪ Developing and applying security system access controls ▪ Deploy, configure and manage encryption/key management services ▪ Establish VPNs ▪ Analyze patterns or trends for further resolution ▪ Manage identity change-request approval processes ▪ Audit, log and report user life-cycle management steps against access control list on managed platforms ▪ Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards and procedures ▪ Complete tasks related to authorization and authentication in physical and logical environments ▪ Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role	
Required qualifications	Education	College diploma in IT field.
	Training	Training in relevant encryption and key management technologies at the applied level.
	Work experience	Experience in managing directory services and working in a security environment.
Tools & Technology	▪ Identity and access management systems ▪ Encryption and key management tools, processes and procedures ▪ VPN and Wi-fi encryption tools and procedures ▪ Authentication tools and services ▪ Security event and incident management systems and/or incident reporting systems and networks	
Competencies	KSAs applied at the basic level:	

	☐ Cryptanalysis ☐ Cryptography and encryption concepts and methodologies ☐ Symmetric and asymmetric cryptography ☐ Steganography and Steganalysis ☐ National cryptologic authorities (Communications Security Establishment) ☐ Public key infrastructure providers KSAs applied at the advanced level: ☐ Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control) ☐ Network access, identity, and access management protocols, tools and procedures ☐ National and international standards ☐ Authentication, authorization, and access control methods ☐ PKI (Public Key Infrastructure), HSM (Hardware Security Module), Digital Certificate, SSL/TLS (Secure Sockets Layer / Transport Layer Security), SSH (Secure Shell), current encryption technologies ☐ Related application life-cycle processes ☐ Digital signatures, digital certificates, and digital certificate management ☐ Authentication protocols ☐ VPN and Protocols ☐ File and Disk Encryption ☐ Encryption Algorithms ☐ Organizational analysis of user and business trends ☐ Client consultation and problem resolution
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their cybersecurity responsibilities relative to organizational cybersecurity risks particularly as they pertain to data encryption requirements. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the cryptographic tools are affected and automated to support organizational requirements. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools to ensure robust cryptographic systems, ciphers and algorithms. If there are known disparities between the threat and the ability to defend, mitigations should be defined and implemented ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will be a need to understand organizational risks posed, measures of security and what policies, processes, or procedures need to be in place. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy within the organization. This includes knowledge and skill of quantum safe algorithms being used, integration and implementation of quantum safe technologies within the

	organization and testing and evaluation protocols for quantum safe/quantum resistant hardware, software, and protocols.