Australian Government

Assessment Requirements for ICTNWK537 Implement secure encryption technologies

Release: 1

Assessment Requirements for ICTNWK537 Implement secure encryption technologies

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- create and document a security plan for the encryption of at least two applications or solutions.

In the course of the above, the candidate must:

- carry out and evaluate encryption of applications or solutions
- analyse enterprise data security requirements
- determine encryption methods.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- industry standard certificate related infrastructure including certificate authorities, registration authorities, repository services
- industry standard symmetric key algorithms and their usage, including:
  - advanced encryption standard (AES), data encryption standard (DES), triple data encryption algorithm (triple DES)
  - Blowfish
- industry standard encryption types, including:
  - public key, secret key, hash key
  - encryption strength
- functions and features of:
  - access control permissions
  - digital signatures and timestamps
  - symmetric encryption, asymmetric encryption and one-way encryption

- one-way message digests including:
  - message digest algorithm 5 (MD5)
  - secure hash algorithm (SHA)
- public key infrastructure (PKI), pretty good privacy (PGP) and GNU Privacy Guard (GnuPG)
- replay security processes and how to prevent them
- transmission control protocol and internet protocol (TCP/IP) protocols and applications
- wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and Wi-Fi protected access 2 (WPA2).

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- a site where encryption installation may be conducted
- a live network
- servers
- industry standard encryption software
- industry standard encryption tools
- organisational security and encryption deliverables.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet - https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2