Specification of Competency Standards for the Retail Industry
Unit of Competency

Functional Area - Transaction Security Technology

Title	Apply encryption technology to send data
Code	107233L4
Description	Apply technical means to change the important information into garbled (encrypted) transmission. Upon reaching the destination, apply the same or different means to restore (decryption).
Level	4
Credit	12 （For Reference Only）
Competency	Performance Requirements 1. Master the basic concepts of encryption technology • Explain the basic terminology of encryption techniques, including: o Plaintext o Ciphertext o Encryption o Decryption o Encryption Algorithm o Decryption Algorithm o Sender o Receiver o Key o Eavesdropper o Cryptanalysis o Cryptanalyst o Passive Attack o Active Attack 2. Apply encryption technology • Apply symmetric encryption technology o Understand the five basic components of symmetric encryption technology ▪ Plaintext ▪ Encryption algorithm ▪ The key ▪ Ciphertext ▪ Decryption algorithm o Understand and select appropriate data encryption algorithms ▪ Data encryption standard (DES) - the most widely used algorithm ▪ Triple DES ▪ Advanced Encryption Standard (AES) ▪ Bluefish algorithm ▪ RC5 algorithm • Apply asymmetric encryption technology o Understand the composition of the public key cryptography system, including: ▪ Plaintext ▪ Encryption algorithm ▪ Public key and private key ▪ Ciphertext ▪ Decryption algorithm o Apply the public key cryptography

Specification of Competency Standards for the Retail Industry Unit of Competency

Functional Area - Transaction Security Technology

	▪ Encryption / decryption: The sender encrypts the message with the recipient’s public key o Digital Signature: The sender signs the message with its private key. The signature can be generated by encrypting the entire message or by encrypting a small piece of information for the message, where the small data block is the function of the entire message ▪ Key exchange: communication exchange key for both parties ▪ RSA algorithm o Recognize other public key encryption algorithms, including: ▪ ELGamal algorithm ▪ Backpack encryption algorithm o Master the key management technology ▪ Key Distribution Technology ▪ Key authentication technology ▪ The Certification Authority (CA) verifies that a public key belongs to a particular entity (A person or a network entity) ▪ Digital certificate • Recognize Secure Sockets Layer (SSL) encryption technology o SSL is a widely implemented public key encryption technology, the main types include: ▪ No client SSL ▪ Configure the clientless SSL for the VPN device ▪ Network to network ▪ Host to network 3. Exhibit professionalism • Introduce the most suitable for the corporate encryption technology. • Abide by professional conduct and prevent any fraud in the use of encryption technology. • Comply with the relevant legal requirements in the use of encryption technology.
Assessment Criteria	The integrated outcome requirement of this UoC is the ability to: • Understand the basic concepts of encryption technology • Master the basic encryption algorithm design principles • Complete the basic encryption calculation and process data transmission.
Remark	