

Specification of Competency Standards
for the Retail Industry
Unit of Competency

Functional Area - Transaction Security Technology

Title	Apply authentication technology and security certification agreement
Code	107234L4
Description	Apply network security authentication technology in the communication between parties for identity confirmation to ensure the safety of communications.
Level	4
Credit	6 (For Reference Only)
Competency	<p>Performance Requirements</p> <p>1. Understand the basic concepts of security authentication technology</p> <ul style="list-style-type: none"> • Confirm whether the certified object is true and effective • By verifying the properties of the object being authenticated, verify that the certified object is valid • Understand the importance of e-business authentication technology <p>2. Master and apply major authentication technology</p> <ul style="list-style-type: none"> • Apply identity authentication technology <ul style="list-style-type: none"> ○ The purpose is to identify the user identity ○ The major methods of applying identity authentication <ul style="list-style-type: none"> ▪ Password - based authentication method ▪ Two-factor certification ▪ Password mechanism ▪ Biometric certification ○ Master the identity authentication protocol system (Kerberos) concept and application methods <ul style="list-style-type: none"> ▪ To a trusted corporate-based authentication agreement, use symmetric cryptography ▪ The complete Kerberos system includes a verification server, a grant server, a web application server, and a network user: <ul style="list-style-type: none"> ▪ The role of the authentication server is to authenticate users and provide access to the license server ▪ The license server is responsible for authorizing the user to issue a license to the user's application server ▪ The web application server provides a server for some type of network application • Apply message authentication technology <ul style="list-style-type: none"> ○ The purpose is to ensure the integrity of information and anti-denial, such as the user to confirm the online information is false, the information is modified by other companies or forged ○ Apply message authentication method <ul style="list-style-type: none"> ▪ Encrypt sensitive files, even if someone intercepts the file cannot get its content. ▪ Ensure the integrity of the data and to prevent the file interceptor to add other information. ▪ Verify the source of the information to ensure the identity of the sender. ○ Select and apply the integrity verification method <ul style="list-style-type: none"> ▪ Apply summary and hash functions ▪ Apply the message digest algorithm MD5 ▪ Master the hash function algorithm SHA-1

Specification of Competency Standards
for the Retail Industry
Unit of Competency

Functional Area - Transaction Security Technology

	<ul style="list-style-type: none"> ○ Determine the security authentication protocol <ul style="list-style-type: none"> ▪ Understand the importance of security certification agreement ▪ Monitor the confidentiality, authenticity, integrity, and non-repudiation of security protocols ▪ Agree on the data encryption model adopted ▪ Agree on the protocol workflow ○ Master the digital signature technology <ul style="list-style-type: none"> ▪ Understand the digital signature definition ▪ Master the main way of signing digital ▪ Understand the scope of digital signature applications <p>3. Exhibit professionalism</p> <ul style="list-style-type: none"> • Ensure compliance with professional conduct and prevent any fraudulent practices in applying certification and safety certification • Ensure compliance with applicable legal requirements in applying certification and safety certification agreements
Assessment Criteria	<p>The integrated outcome requirement of this UoC is the ability to:</p> <ul style="list-style-type: none"> • Understand the basic concepts of authentication and security authentication protocols. • Master the basic authentication technology and safety certification agreement design principles. • Properly select and apply appropriate certification and safety certification agreements to ensure data security.
Remark	