Certification from SWIFT

The ultimate validation of skills

- How do you demonstrate to prospective employers that you are a true SWIFT Expert?
- How do you really know the SWIFT knowledge of candidates?
- Want to get ahead in your career?

Topic	SWIFT Certified Expert – SWIFTNet Security Officer
Aim	Individuals who successfully pass this certification exam understand the responsibilities and tasks required of a designated Security Officer in their organisation.
Content	SWIFTNet Security Officer Environment
	Certificate Management
	Connectivity and Security
	SWIFTNet Online Operations Manager
	Reporting
	RBAC Roles
	Secure Channel
	SWIFTNet Naming
	SWIFTNet Security Officer Tasks
	SWIFTNet PKI
Target Audience	New and experienced SWIFTNet Security Officers. SWIFT Partners and service bureaux are not eligible to the Programme.
Recommended Study SWIFTSmart Curriculas:	SWIFTNet Security Officer - Associate
	SWIFTNet Security Officer - Professional
	SWIFTNet Security Officer - Expert
	Customer Security Program - All modules
Experience	No specific experience is necessary
Exam Method	A variety of multiple-choice questions and situational scenarios
	Proctored exam - on-site as part of tailored training event or online via SWIFTSmart
Fee	Certification fee + Proctoring fee
Validity	Two years

As SWIFT certification is based on transparency, exam criteria is detailed below to help ensure you are fully prepared.

Exam questions may additionally test your ability to apply knowledge and theory to relevant situational scenarios.

In order to successfully pass the exam you need to be able to:

SWIFTNet Security Officer Environment

List at least three benefits of the VPN boxes as part of the Network security Layer

List the two portals a SWIFTNet Security Officer can use to manage digital entities

List at least three benefits of the Messaging security Layer

List at least three benefits of the Application security Layer

Recall the purpose of a Closed User Group (CUG)

List at least three value-added-services that are provided by SWIFT as part of the Message security Layer

Recall the three types of cryptography is used in SWIFT's infrastructure

Recall at least three locations in the local SWIFT infrastructure where a customer can store PKI certificate private keys

Certificate Management

Remember the signing keys expiration period for user business certificates

Recall at least two outcomes that occur as the result of the expiry of user business certificate's private key

Recall the User certificate class used to sign production traffic

Recall the three steps that you must take if a PKI certificate has expired, and you do not want to use it again

Recall the steps that you must take if a PKI certificate has expired, and you do want to use it again

Recall at least three valid certificate statuses to be able to perform a certificate recovery

Recall when the renewal period begins for user certificates

Recall the steps to manually renew an expired certificate

Remember the two types of user password policy

List at least the three actions required to remove an entity from the DN tree

Recall the time-period between performing a deletion action and the removal of the entity from the DN tree

Recall at least two valid user statuses where a deletion action can be performed on an entity in the DN tree

Recall at least three characteristics of the password policy of a human-owned certificate

Recall at least three characteristics of the password policy of an application-owned certificate

Connectivity and Security

Recall the purpose of the Network security Layer

Recall at least two locations where PKI secrets are stored locally on a customer site

Recall where the private keys of a SWIFTNet Link certificate are stored in a typical customer's SWIFT environment

Recall the purpose of the Messaging security Layer

Recall the purpose of the Application security Layer

SWIFTNet Online Operations Manager

Recall at least three certificate management tasks that can be performed using the SWIFTNet Online Operations Manager

Recall two requirements to accessing the SWIFTNet Online Operations Manager using WebAccess

Recall at least three types of entity that can be viewed in the DN tree in the SWIFTNet Online Operations Manager

Recall the outcome of trying to send a message over the SWIFT network with a revoked certificate

Recall the outcome of deleting a registered e-mail in the SWIFTNet Online Operations Manager

Recall the steps to take to protect your company if an end user with an anonymous (PKI) Test / Pilot certificate leaves the company

Recall the steps to take to protect your company if an end user with a personal nominal (PKI) certificate leaves the company

Remember the purpose of the E-mail Registration menu in the Administration section of the SWIFTNet Online Operations Manager

Remember the purpose of the activation code that is generated during the registration process of a new e-mail address in the SWIFTNet Online Operations Manager

Recall how the activation code generated during the registration process of a new e-mail address in the SWIFTNet Online Operations Manager is received and used

Reporting

Recall the report in the SWIFTNet Online Operations Manager that displays all changes related to certificate management

Recall the SWIFT service name to receive automated reports through FileAct

Remember how SWIFTNet security officers assign RBAC roles in the SWIFTNet Online Operations Manager

Name the two options available for the channel pane of an automated report in the SWIFTNet Online Operations Manager

Recall at least four certificate types that can be chosen when running a certificate report

Remember at least three types of information that is included in an Activity Log report generated in the SWIFTNet Online Operations Manager

Remember at least three types of information that is included in a Role report generated in the SWIFTNet Online Operations Manager

Recall the three reports that can be run in the SWIFTNet Online Operations Manager

Recall at least three search criteria in the SWIFTNet Online Operations Manager that you can select for a Certificate Report

List at least three purposes for reports

List at least three ways to generate and receive reports in the SWIFTNet Online Operations Manager

RBAC Roles

Recall the two functions that can be used to assign roles to multiple users in the SWIFTNet Online Operations Manager

Remember at least four steps that are required to assign RBAC roles in the SWIFTNet Online Operations Manager

Name two actions in the SWIFTNet Online Operations Manager to make the process of assigning roles to multiple users more efficient

Recall the purpose of RBAC roles

Recall the purpose of Basic and Extended RBAC roles

Recall the RBAC role that enables a SWIFTNet security officer to a register an entity and manage its certificates in 2-eyes

Recall at least three aspects of certificate management in the SWIFTNet Online Operations Manager when the SWIFTNet security officers are using the 4-eyes principle

Recall how an institution can control access of its individuals and applications to specific parts of a service

Secure Channel

Name at least two items required to activate a Secure Code Card

List at least three tasks that an offline SWIFTNet security officer can perform on Secure Channel

Recall the type of SWIFTNet security officer who is only known to their institution, and not to SWIFT

List at least three actions that an offline SWIFTNet security officer can perform on the Secure Code Card

Remember the first step that a SWIFTNet security officer must take when they receive their Secure Code Card before it can be used

Recall the type of SWIFTNet security officer who is known to both their institution and to SWIFT

Remember the status of the Secure Code Card in Secure Channel when a SWIFTNet security officer first receives it

SWIFTNet Naming

Recall which levels of the SWIFTNet PKI tree are created by SWIFT

Recall at least three naming conventions you must follow when creating a Distinguished Name

Remember the number of SWIFTNet security officers required per location in a 4-eyes configuration

Recall the purpose of the SWIFT.LRA//CertificateAdministration role

Recall the purpose of the SWIFT.RBAC//Delegator//SWIFT.LRA//CertificateAdministration role

Recall the purpose of Federated DNs

List the two categories of name addressing in SWIFTNet

SWIFTNet Security Officer Tasks

Recall at least three SWIFT security profiles

Name at least three best practice security officer tasks

List at least four scenarios where you must perform a certificate recovery to resolve

List at two reasons why there could be a limitation to what you can manage in your PKI tree using the SWIFT Online Operations Manager

Recall when a deletion request is made on an entity, how long it takes before the entity is removed from the PKI tree

Remember the steps to create a back-up certificate for your SWIFTNet security officer on your Disaster Recovery which uses its own HSM cluster

Recall at least one scenario where SWIFTNet security officers use the Local Registration Authority

Name the two authorisation options that an institution may have for offline security requests

List at least two certificate administration tasks performed by an Alliance Gateway Administrator

Recall the name of the online tool used when setting up additional SWIFTNet security officers

Name the two tools the SWIFTNet security officers can use to revoke certificates

Explain the dual authorisation principle

Describe what an administering institution is

Explain the role of the SWIFTNet Certification Authority when a certificate is revoked

List at least two tasks performed by the swift.com Administrator

Recall the minimum number of SWIFTNet security officers that an institution can have
Recall if and who a SWIFTNet security officer can share their Secure Code Card with
SWIFTNet PKI
Name two types of certificate that can be used to send traffic for a pilot service
List the three types of certificate that can be managed using the Online Operations Manager
List at least three components of a SWIFTNet User certificate
Recall two purposes of public key pairs
List at least three classes of User Certificate
Recall two purposes of the SWIFTNet Certification Authority
Recall two purposes of private key pairs
Recall two uses of certificates signed by the SWIFTNet Certification Authority
Recall the three benefits of digitally signing your SWIFT messages
Recall the purpose of the digital certificate in SWIFTNet
Explain the signing and verification process on SWIFTNet
Recall the benefit of digitally encrypting data that you exchange over the SWIFT network
Recall the type and class of certificate used to sign traffic for a Live service
Recall how private keys must be stored
Describe the purpose of SWIFTNet PKI
Recall how public keys are stored
Describe the PKI process and which keys are used by your correspondent to confirm that a SWIFT message has come from you

For more information about SWIFT,
visit www.swift.com