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
	Monitoring
	Online Operations Manager
	Routing Rules and Reporting
	RBAC Roles
	Secure Channel
	SWIFTNet Naming
	Security Officer Tasks
	SWIFTNet PKI
Target Audience	New and experienced Security Officers
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 the five messaging services offered by SWIFT

Describe the SWIFT messaging services that can be used to exchange images and PDF documents

Recall the Swift messaging service that allows you to send hundreds of transactions per second

Describe the four categories of SWIFT software solutions

List the key differences between 'SWIFT Cloud' and 'On Premises' solutions

List the two components that are replaced when using ARG

List at least two uses of the Alliance Integration Platform (IPLA)

List at least one use of Alliance Integration Platform (SIL)

Certificate Management

Explain the difference between the two Certificate Types when creating a certificate in Online Operations Manager

Name the Certificate Class for certificates used to sign production traffic

Describe the two password policies available when creating a certificate in Online Operations Manager

List at least two reasons why a certificate might become unusable

List at least two occasions when the Recovery option in Online Operations Manager should be used for a given certificate

Describe the purpose of the Activations Secrets feature in Online Operations Manager

Explain the impact on the message flow of the SNL certificate recovery procedure

Demonstrate how to setup at least one SNL certificate for recovery in Online Operations Manager

Demonstrate how to recover at least one SNL certificate in the SWIFTNet link command prompt

Demonstrate how to certify a new Security Officer using Alliance Gateway

Explain the purpose of the Relaxed option when certifying /recovering a certificate in Alliance Gateway

Demonstrate how to certify a new application certificate using Alliance Gateway

Demonstrate how to recover a Business certificate using Alliance Gateway

Connectivity and Security

List the two components of the SWIFT On Premises connectivity solution

List the three security layers of the SWIFT SIPN

Identify where a PKI certificate for the application layer is stored

Identify where an SNL certificate is stored

Explain the three fundamental drivers of the SIPN

Recall at least two components of the Managed Customer on Premises Equipment (MCPE)

List three methods how the SNL secures the Messaging layer

List at least three methods how the VPN secures the IP layer

Monitoring

Demonstrate how to view the number of transactions per second (TPS) for FIN, InterAct and FileAct traffic

Demonstrate how to generate a TPS report and export it to a CSV file

List two possible outputs on the CSV report when no traffic data is available

List the two options available to measure traffic volume in Online Operations Manager

Demonstrate how to generate a count report and export it to a CSV file

Demonstrate how to see the Queue Status Information for SWIFTNet in Online Operations Management

Demonstrate how to see the Queue Status Information for FIN in Online Operations Management

Online Operations Manager

List at least three tasks that can be carried out using WebAccess

List the three main benefits of using WebAccess

Recall the SWIFT messaging service which allows members to access financial online portals

Describe the primary use of Alliance Web Platform

List at least two uses of Online Operations Manager

Recall at least four best practices for Online Operations Manager

Demonstrate how to access SWIFTNet Online Operations Manager from Alliance Web Platform

Demonstrate how to register an email in Online Operations Manager

Recall at least three implications of deleting a registered email in Online Operations Manager

Routing Rules and Reporting

Recall the three steps to setup certificate report in Online Operations Manager

Demonstrate how to create a certificate report in Online Operations Manager

Demonstrate how to setup an automated report in Online Operations Manager

Demonstrate how to create a role report in Online Operations Manager

Demonstrate how to create an Activity Log report in Online Operations Manager

List the four components of a routing rule

Explain the difference in the delivery endpoint between a real-time service and a store-and-forward service

Identify where SWIFT stores routing rules

Demonstrate how to search for a routing rule

Demonstrate how to enable/disable a routing rule

Demonstrate how to reroute at least one routing rule

RBAC Roles

List at least three uses of a CUG in relationship with RBAC

Recall the two ways RBAC can be implemented as a service

Identify who manages the RBAC roles for a service

Identify who assigns the RBAC roles for an institution

Recall the five steps involved in the activation of RBAC

List at least two Security Officer roles specific to certificate management

List at least four Security Officer roles specific to role management

Describe the use of the ServiceUser role

List at least two options available in Online Operations Manager to manage RBAC roles

Explain at least two differences in how roles are assigned between live and pilot services

Demonstrate how to assign and RBAC role in Online Operations Manager

Describe the purpose of the "swift.snf.control" role given to a certificate

List two features of managing role delegation in Online Operations Manager

Demonstrate how to grant roles to several users at once in Online Operations Manager

Demonstrate how to copy roles from a user in Online Operations Manager

List the four RBAC roles needed for email registration

Secure Channel

Define the purpose of the Secure Channel

Recall at least two best practice tips for using Secure Channel

Demonstrate how to submit a Secure Channel request and download the activations codes

Demonstrate how to revoke a Security Officer Secure Code Card

Demonstrate how to activate a Security Officer secure code card

SWIFTNet Naming

Differentiate the use of the BIC Directory and SWIFTNet Directory

Recall the use of levels on a SWIFTNet PKI Tree

Recall the use of the Primary BIC (BIC8)

Describe the 2 categories of name addressing

Describe the hierarchical structure of the Distinguished Name (DN)

List the two parts of the SWIFTNet PKI tree that are created by SWIFT

Recall the number of DN levels recommended by SWIFT

Name the use of the "swift.fin" role given to a certificate

List the two roles required to assigned the "swift.fin" role to a certificate

Recall three segments that compose a DN

Recall at least three restrictions on the naming format of a DN

Recall at least one characteristic of the naming convention for a Web Certificate

Security Officer Tasks

Name the online and offline tools to manage security aspects by SWIFTNet Security Officers

Explain the two authorisation principles

Describe at least four tasks carried out by a Security Officer

Explain the authentication methods used for both online and offline Security Officer

Recall at least three general recommendations for a Security Officer

Define a shared Security Officer

Define the minimum number of Security Officers on each organisation

Explain the difference between a SWIFTNet Security Officer and a Customer Security Officer

List the three administrative tasks a Security Officer can do with a certificate

Identify how to access the Online and Offline tools for a Security officers

Recall at least four SWIFT Security Profiles of a fully on premises infrastructure

Match at least four SWIFT Security Profiles with their corresponding task in a fully on premises infrastructure

List the three SWIFT Security Profiles available for an organization connected through Alliance Remote Gateway

Match at least two SWIFT Security Profiles with their corresponding task in an on premises infrastructure

List the two SWIFT Security Profiles in a fully cloud infrastructure (Alliance Lite2)

Match the two SWIFT Security Profiles with their corresponding task in an on premises infrastructure

List the three main tasks completed by a swift.com administrator

SWIFTNet PKI

Recall the type of cryptography used by the SWIFTNet PKI

Describe the purpose of the SWIFTNet PKI

List the four activities which the SWIFTNet Certification Authority is responsible for

Name the two uses of a certificate signed by the SWIFTNet Certification Authority

Identify at least four components of the SWIFTNet Certification Authority signature

List the two uses of the private key pairs

Recall two uses of the public key pairs

Indicate where a private key and a public key should be stored

Compare private keys with public keys

List the three benefits of signing data

Illustrate how the signing and verification cycle work

Name the benefit of encrypting data

Illustrate how the encryption and decryption cycle work

Recall the three types of certificates that can be managed using Online Operations Manager

List at least three certificate classes that can be managed using Online Operations Manager

Describe the two types of InterAct and FileAct certificates

Describe the use of the end-to-end signature

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