SWIFT

SWIFT Qualified Certificates

Certificate Policy

This *Certificate Policy* applies to Qualified Certificates issued by SWIFT. It indicates the requirements and procedures to be followed, and the responsibilities of the parties involved, during the lifecycle of the Certificates in accordance with the *SWIFT Qualified Certificates Certification Practice Statement*. This document is effective from 6 December 2013.

22 November 2013

Table of Contents

Preface

Purpose of this document

This *Certificate Policy* applies to Qualified Certificates issued by SWIFT. It indicates the requirements and procedures to be followed, and the responsibilities of the parties involved, during the lifecycle of the Certificates in accordance with the *SWIFT Qualified Certificates Certification Practice Statement*.

1 INTRODUCTION

A Certificate Policy is a set of rules, requirements, and definitions determining the level of assurance provided by a determined type of Certificate, and its applicability to a particular community and/or class of applications with common security requirements. Different levels of assurance may correspond to different Certificate Policies and different types of Certificates. Certificates issued in accordance with a determined Certificate Policy include a Certificate Policy identifier, a unique number called “Object Identifier” (OID), which can be used by Relying Parties to determine Certificate suitability for a particular application.

SWIFT registers its Certificate Policy Object Identifiers under the root "1.3.21.6".

1.1 Overview

The present document is the Certificate Policy titled “SWIFT Qualified Certificates – Certificate Policy”. It applies to Qualified Certificates issued by SWIFT. Qualified Certificates are defined in the EU Directive 1999/93/EC on a Community framework for electronic signatures[1]. The present *Certificate Policy* indicates the requirements and procedures to be followed, and the responsibilities of the parties involved, during the lifecycle of the Certificates in accordance with the *SWIFT Qualified Certificates Certification Practice Statement* [1].

Every SWIFT Qualified Certificate issued under this *Certificate Policy* will carry a Certificate Policy OID corresponding to the assurance level of that Certificate as stated in section 1.2 and to the rules, requirements and definitions applicable as per the present *Certificate Policy*.

"SWIFT Qualified Certificates" are issued to Subscribers and are typically for use in conjunction with specific SWIFT services and products requiring such Qualified Certificates. The creation of the keys is performed by the Subscriber, the key-size is 2048 bit, the corresponding private key resides in an HSM, and the validity period is 2 years.

SWIFT Qualified Certificates issued under this *Certificate Policy* provide assurance of the identity of the Subscriber as further described in this *Certificate Policy*.

1.2 Document Name and Identification

This *Certificate Policy* document is named: "SWIFT Qualified Certificates Certificate Policy".

This document is structured according to the framework defined in IETF RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

By including the following unique Object Identifier in its SWIFT Qualified Certificates, SWIFT guarantees its conformance with the Certificate Policy requirements as described in the present document.

Name of Certificate Type	Object Identifier
SWIFT Qualified Certificate	1.3.21.6.3.10.200.3

[1] The European Directive 1999/93/EC of the European Parliament and the Council of the 13 December 1999 on a Community framework for electronic signatures. O.J. L 13, 19.1.200, p.12.

1.3 PKI Participants

In the context of issuing SWIFT Qualified Certificates, SWIFT is acting as the Certification Service Provider. As Certification Service Provider, SWIFT has final and overall responsibility for the provision of the SWIFT Qualified Certificates offering, namely the Certificate generation services through the SWIFTNet PKI Certification Authority, the registration services through the SWIFTNet PKI Registration Authority, the Revocation Management Services, the Revocation Status Information Service (providing Certificate validity status information), and the Dissemination Services. Other PKI participants are the Subject Device (HSM) Provisioning Services, the Subscribers, and the Relying Parties.

All communications between certification component service providers regarding any phase of the lifecycle of the Certificates are secured with PKI-based encryption and signing or strong authentication techniques (PKI-based or not) to ensure confidentiality, mutual authentication and secure logging/auditing.

1.3.1 Certification Authorities

SWIFT operates the SWIFTNet PKI CA, the Certification Authority which issues the SWIFT Qualified Certificates that are ruled by this *Certificate Policy*.

1.3.2 Registration Authorities

SWIFT operates the SWIFTNet PKI RA, the Registration Authority of the SWIFTNet PKI in the context of issuing the SWIFT Qualified Certificates.

1.3.3 Subscribers

Subscribers of SWIFT Qualified Certificates are those organisations that contract with SWIFT for the issuance of a SWIFT Qualified Certificate in their name. Typically, Subscribers are SWIFT users that require a SWIFT Qualified Certificate to sign messages or files sent over SWIFT.

1.3.4 Relying Parties

The Relying Parties are those persons who are relying on a SWIFT Qualified Certificate by verifying the signature of a Subscriber.

1.3.5 Other Participants

SUBJECT DEVICE PROVISIONING SERVICES

The Secure Subject Devices required to contain the private key corresponding to the SWIFT Qualified Certificate (the Hardware Security Module, HSM) are provided to the Subscribers by SWIFT. The creation of the Certificate key pair is performed by and under sole control of the Subscriber, the private key is generated in the HSM and cannot be exported in clear text form.

DISSEMINATION AND REPOSITORY SERVICES

SWIFT is operating the Dissemination Services (publication of Certification Practice Statement, Certificate Policy, General Terms and Conditions, CA certificate, and other related, public documents). These services are available from http://www.swift.com/pkirepository. This interface also provides access to former versions of these documents (Certification Practice Statement, Certificate Policy, General Terms and Conditions).

Access to CRLs, CA Certificates, Certificates download, Certificates status is provided through the SWIFT network and related hardware and software configuration required for SWIFT connectivity. A combined CRL is also publicly available from https://www2.swift.com/pkirepository/SWIFTCA.crl.

Dissemination and Repository Services are provided as described in section 2 of the present *Certificate Policy*.

REVOCATION MANAGEMENT SERVICES AND REVOCATION STATUS INFORMATION SERVICES

SWIFT is operating the Revocation Management Services and the Revocation Status Information Services (which provide Certificate validity status information) with regards to the SWIFT Qualified Certificates that are ruled by this *Certificate Policy*.

Revocation of a SWIFT Qualified Certificate can be requested by the Subscriber to which the Certificate is issued, as well as by SWIFT as Certification Service Provider, as ruled by the present *Certificate Policy* (see section 4.9.1).

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

SWIFT QUALIFIED CERTIFICATES

These Certificates have a Policy OID 1.3.21.6.3.10.200.3.

"SWIFT Qualified Certificates" are issued to Subscribers as defined in section 1.3.3. The creation of the keys is performed by the Subscriber, the key-size is 2048 bit, the corresponding private key is generated in, and resides in, an HSM (and cannot be exported in clear text form), and the validity period is 2 years.

The Certificates issued under this *Certificate Policy* provide assurance of the identity of the Subscriber, and are typically for use in conjunction with specific SWIFT services and products requiring such Qualified Certificates.

The permitted usage of a SWIFT Qualified Certificate is limited to the support of electronic signatures and non-repudiation. See section 7.1 for more information on the KeyUsage definition of a SWIFT Qualified Certificate.

The Subscriber is identified through an ISO 9362 Business Identifier Code (BIC) in the Certificate Subject field.

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

The SWIFTNet PKI Policy Management Authority (PMA) consists of different complementary organisational entities and working groups within SWIFT or other entities in the SWIFT group, managing the SWIFTNet PKI service.

The SWIFTNet PKI PMA has the responsibility for continually and effectively managing SWIFTNet PKI related risks. This includes a responsibility to periodically re-evaluate risks to ensure that the controls that have been defined remain appropriate, and a responsibility to periodically review the controls as implemented, to ensure that they continue to be effective. This is covered by the Information Security Risk Management framework at SWIFT.

1.5.2 Contact Person

All questions and comments regarding this *Certificate Policy* should be addressed to the representative of the SWIFTNet PKI Policy Management Authority:

SWIFT SCRL – ITOPS – Enterprise Security & Architecture
Avenue Adele 1
1310 La Hulpe
Belgium

Tel: +32 2 655 33 32 - E-mail: swift-pma@swift.com

1.5.3 Person Determining CPS Suitability for the Policy

The SWIFTNet PKI Policy Management Authority (PMA) determines CPS suitability for the present *Certificate Policy*. This determination is limited to the *SWIFT Qualified Certificates Certification Practice Statement* [1].

1.5.4 Approval Procedures

The SWIFTNet PKI Policy Management Authority (PMA) approves this document and any subsequent changes.

The existing SWIFT Change Control mechanism will be used to trace all identified changes to the content of this document. Changes considered as minor will be clearly labelled, making it possible to identify which version of this *Certificate Policy* is applicable to SWIFT Qualified Certificates issued at a given time. Changes considered as major will initiate the creation of a new Certificate Policy OID and documented as such.

Comments, questions, and change requests to this *Certificate Policy* document should be addressed to the SWIFTNet PKI Policy Management Authority specified in section 1.5.2 - Contact Person.

This *Certificate Policy* shall be reviewed in its entirety every year or when major SWIFTNet PKI releases are implemented. Errors, updates, or suggested changes to this document shall be communicated to the SWIFTNet PKI Policy Management Authority.

1.6 Definitions and Acronyms

Terms	Definitions
Activation Data	Data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.
Certificate	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
Certificate Generation Activation Secrets	Data values that are required to initiate the certification process, and that link the Certificate registration with the actual Certificate issuing.
Certificate Revocation List	A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is made available by the SWIFTNet PKI CA to Subscribers and Relying Parties. The CRL is updated after each Certificate revocation process. The CRL does not necessarily contain identifiers of revoked Certificates that are past their validity date (that is, expired). SWIFTNet PKI provides both partitioned CRLs and a combined CRL. Partitioned CRLs contain information on a specific subset of revoked SWIFT Qualified Certificates. Each SWIFT Qualified Certificate indicates in which partitioned CRL its revocation information can be found. The combined CRL contains information on all revoked SWIFT Qualified Certificates.
HSM	Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
Qualified Certificate	A Certificate which meets the requirements laid down in Annex I of EU Directive 1999/93/EC and is provided by a Certification Service Provider who fulfils the requirements laid down in Annex II of that Directive
Relying Party	Person or organisation acting upon a Certificate, typically to verify signatures by the Subscriber or to perform encryption towards the Subscriber. The Relying Party relies upon the accuracy of the binding between the Subscriber public key distributed via that Certificate and the identity and/or other attributes of the Subscriber contained in that Certificate. In the context of this *Certificate Policy* for SWIFT Qualified Certificates, Relying Parties are as further defined in section 1.3.4.
Subscriber	Person or organisation contracting with the Certification Authority, for being issued one or more Certificates. In the context of this *Certificate Policy* for SWIFT Qualified Certificates, the Subscribers are as further defined in section 1.3.3.
SWIFT	S.W.I.F.T. SCRL
SWIFTNet Directory	The SWIFTNet Directory is a centralised X.500 directory of entities that stores the Certificates and Certificate Revocation Lists that the Certification Authority issues. The SWIFTNet Directory identifies an entity by its Distinguished Name (DN).

Terms	Definitions
SWIFTNet PKI	The pervasive SWIFT security infrastructure that provides digital signatures and the supporting certification services based on public key cryptography. The SWIFTNet PKI service comprises the SWIFTNet PKI CA, the SWIFTNet PKI RA and the SWIFTNet Directory, which provide the PKI participants with online Certificate management capabilities.
SWIFTNet PKI CA	The SWIFTNet PKI Certification Authority, operated by SWIFT, creates and manages Certificates for Entities that have been registered by the SWIFTNet PKI Registration Authority.
SWIFTNet PKI RA	The SWIFTNet PKI Registration Authority, operated by SWIFT

Acronym	Definition
ARL	Authority Revocation List
BIC	Business Identifier Code
CA	Certification Authority
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
HSM	Hardware Security Module
KMA	Key Management Application
LSO	Local Security Officer
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The SWIFTNet Directory is a centralised X.500 directory of entities that stores the Certificates and Certificate Revocation Lists that the Certification Authority issues. An Authority Revocation List (ARL) is published in the SWIFTNet Directory. The SWIFTNet Directory identifies an entity by its Distinguished Name (DN).

The *SWIFT Qualified Certificates Certification Practice Statement* [1] is available online on http://www.swift.com/pkirepository. This repository shall also contain other public documents related to the issuance of SWIFT Qualified Certificates, such as the present *Certificate Policy*, the *SWIFT Qualified Certificates Terms and Conditions*, and the SWIFTNet PKI CA public key certificate.

A combined Certificate Revocation List (CRL) is available on https://www2.swift.com/pkirepository/SWIFTCA.crl.

2.2 Publication of Certification Information

SWIFTNet PKI CA publishes Certificates and Certificate Revocation Lists (CRLs) in the SWIFTNet Directory. A combined Certificate Revocation List (CRL) is also publicly available on https://www2.swift.com/pkirepository/SWIFTCA.crl.

SWIFTNet PKI CA removes expired Certificates from its Certificate Revocation Lists.

2.3 Time or Frequency of Publication

New CRLs are created either every 24 hours by the re-signing of existing CRLs or immediately after a Certificate revocation. The new CRL(s) are published in the SWIFTNet Directory immediately following creation, and will be available for Relying Parties to download within 7 minutes after creation. The combined CRL available on https://www2.swift.com/pkirepository/SWIFTCA.crl is published every 24 hours.

Certificates are published in the SWIFTNet Directory immediately after creation. Expired Certificates are removed from the SWIFTNet Directory when a new Certificate is issued to the same Subject Distinguished Name (DN) as described in sections 3.3 and 4.7 on Certificate Re-Key.

Updates to the present *Certificate Policy*, the *SWIFT Qualified Certificates Certification Practice Statement* [1], the *SWIFT Qualified Certificates Terms and Conditions*, and other public documents are published whenever a change occurs, ensuring a period of minimum fourteen (14) calendar days between the publication date and the effective date (see section 9.12).

2.4 Access Controls on Repositories

The Certificates and Certificate Revocation Lists are available to security officers through SWIFTNet Link.

The Subscribers and Relying Parties have **Read** access to the Certificates and CRLs in the SWIFTNet Directory.

Write access to the Certificates and CRLs in the SWIFTNet Directory is restricted to the SWIFTNet PKI CA.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The SWIFT Qualified Certificates are issued to Subscribers as defined in section 1.3.3. A Subscriber is identified by a Business Identifier Code (BIC), which is a standardized (ISO 9362) identifier for financial and non-financial institutions to facilitate automated processing of telecommunication messages in banking and related financial transaction environments.

SWIFT Qualified Certificates have a Subject Distinguished Name (DN) with the pattern
cn=%<number>,cn=Qualified Enterprise,o=<BIC>,o=swift

in which the *cn=%<number>* part is optional, and <*number*> is a numeric string with a maximum length of 8 digits.

The element representing the identity of the Certificate's Subject is the o=<*BIC*>, appearing in second level after root o=swift.

The optional cn=%<*number*> part allows the Subscriber to handle multiple SWIFT Qualified Certificates in its organisation.

SWIFT Qualified Certificates are issued by the SWIFTNet PKI CA, which has a self-signed CA Certificate issued to Subject "o=swift", and is hence also the Root CA and Trust Anchor in the SWIFTNet PKI.

SWIFT Qualified Certificates include Certificate extension "Issuer Alternative Name" to indicate the name of the Certification Service Provider organisation as stated in the official records, and the country in which it is established, as "cn=SWIFTNet PKI CA,o=S.W.I.F.T. SCRL,c=BE".

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The possession of the private key for SWIFT Qualified Certificates issued by the SWIFTNet PKI CA is verified by validating the digital signature during a "proof-of-possession" PKIX-CMP[2] exchange.

3.2.2 Authentication of Identity

SWIFT QUALIFIED CERTIFICATE – REGISTRATION PROCESS

Prerequisites:

The SWIFTNet PKI CA issues SWIFT Qualified Certificates to Subscribers as defined in section 1.3.3. Therefore, an organisation requesting a SWIFT Qualified Certificate, must fulfil the necessary prerequisites to obtain SWIFT network connectivity. This includes setting up a hardware and software configuration that allows connectivity on SWIFTNet, and offers a strong authentication mechanism, strong confidentiality and integrity protection, and a trusted communication channel for the Subscriber to communicate with SWIFT.

As part of its configuration, the Subscriber defines at least two "Local Security Officer" (LSO) accounts that are entitled to manage the Subscriber's SWIFTNet configuration. The Subscriber can choose to work in a dual authorisation mode, in which a second LSO account needs to approve the configuration change introduced by a first LSO account.

[2] Certificate Management Protocol, RFC 4210

The LSO accounts are entitled by the Subscriber to manage its Qualified Certificate. The LSO accounts are defined as part of the SWIFT network connectivity setup. The LSO accounts must belong to the Subscriber organisation. Section 4.1.2 elaborates this process.

The identity validation process involves the verification by SWIFT of the identity of the Subscriber and the identity of a natural person representing the organisation. SWIFT will ask the Subscriber to provide identity information and supporting documents as required to perform the identification. The identification is based on documents that are applicable in the local country, such as a valid Certificate of Incorporation, and a valid personal identification document. SWIFT stores the identification documents and retains this information for the required period (30 years).

Identification and authentication procedures for registration by the SWIFTNet PKI RA are detailed in SWIFT internal documents (*QC Customer Identification* process).

3.3 Identification and Authentication for Re-key Requests

Certificate renewal as defined in PKI standards, that is, issuing a new Certificate to an existing key pair, is a functionality that is not implemented by the SWIFTNet PKI.

Subscribers that need to renew their Certificates shall also be required to generate new key pairs (known as re-key).

Re-key requests are considered to be new Certificate requests. Before such new Certificates are issued, the identity of the Subscriber and representing natural person will be re-verified as described in section 3.2.2 on Initial Identity Validation. Updated or new identification documents are added to the customer information file and retained for the required period (30 years).

3.3.1 Identification and Authentication for Routine Re-key

The same process as for Initial Identity Validation is used (section 3.2.2).

3.3.2 Identification and Authentication for Re-key after Revocation

The same process as for Initial Identity Validation is used (section 3.2.2).

3.4 Identification and Authentication for Revocation Request

The LSO accounts are entitled by the Subscriber to which they belong to manage its Qualified Certificate, including revocation. The LSO accounts are defined as part of the SWIFT network connectivity setup.

Identification and authentication procedures for revocation by the Certification Authority (for reasons discussed in section 4.9.1) are detailed in SWIFT internal documents.

4 CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

A SWIFT Qualified Certificate can be requested by a Subscriber "Local Security Officer" account. The LSO accounts are mandated by the Subscriber, as discussed in section 3.2.2.

4.1.2 Enrolment Process and Responsibilities

The LSO account as registered with SWIFT and entitled by the Subscriber to manage its SWIFT Qualified Certificate, uses the "Secure Channel" application to communicate with the RA, and request a SWIFT Qualified Certificate.

The Subject DN for a SWIFT Qualified Certificate has a fixed structure per Subscriber, as described in the "Naming" section 3.1 above. The LSO account submits a request for Certificate issuing to the SWIFTNet PKI RA using the "Secure Channel" application. As part of preparing the request, the LSO account defines a download password that is used in a later phase of the process. If the Subscriber requires dual authorisation, a second LSO account must confirm this request.

This request to issue a SWIFT Qualified Certificate must be performed no later than 3 months after the successful completion of the identity validation process (described in section 3.2.2).

The SWIFTNet PKI RA registers the Subject DN in the PKI, defines the Certificate parameters, and configures it to be ready for certification. This results in the generation of "certificate generation activation secrets", which are made available to the LSO account for secure download – using the download password defined previously.

The LSO account subsequently downloads the certificate generation activation secrets. Further use is described in section 4.3.

The procedures for the enrolment process by the SWIFTNet PKI RA are detailed in SWIFT internal documents.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The Subscriber and its LSO accounts are defined as part of the SWIFT network connectivity setup, as described in section 3.2.2. The LSO accounts have a secure communication channel with SWIFT called "Secure Channel", in which their identity is strongly authenticated.

4.2.2 Approval or Rejection of Certificate Applications

Not applicable.

4.2.3 Time to Process Certificate Applications

SWIFTNet PKI RA will process the Certificate application on Belgian business days. The notification towards the LSO account that the certificate generation activation secrets are available is sent the next Belgian business day.

4.3 Certificate Issuance

As described in section 4.1.2, the LSO account receives certificate generation activation secrets after having requested a SWIFT Qualified Certificate to the SWIFTNet PKI RA.

As described in section 3.2.2, the Subscriber must have set up a hardware and software configuration that allows connectivity on SWIFTNet. To obtain a SWIFT Qualified Certificate, the Subscriber must use this SWIFTNet connectivity, in particular the Key Management Application (KMA) available on the SWIFTNet Link interface.

The KMA generates the public and private key pair on an HSM connected to the SWIFTNet Link. KMA requires the LSO account to supply the certificate generation activation secrets, and sends these together with the public key to the SWIFTNet PKI CA. The exchange between the KMA and the SWIFTNet PKI CA is based on the PKIX-CMP protocol.

The SWIFTNet PKI CA validates the certificate generation activation secrets, and generates the Certificate with the Certificate parameters provided by the SWIFTNet PKI RA as described in section 4.1.2.

The certificate generation activation secrets remain valid during 180 days, but can only be used once.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

By using the certificate generation activation secrets in the Key Management Application, the Certificate is automatically generated and accepted.

4.4.2 Publication of the Certificate by the CA

The Certificate is published by the SWIFTNet PKI CA to the SWIFTNet Directory.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The key pairs associated to SWIFT Qualified Certificates are generated and stored in a Hardware Security Module (HSM) by the Subscriber and under its sole control.

Access to the private key in the HSM is protected with a password, which is chosen by the Subscriber and which must be compliant to the password policy imposed by the Key Management Application (see *SWIFT Qualified Certificates Certificate Administration Guide* [3]).

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties should not rely on SWIFT Qualified Certificates issued in accordance with the present *Certificate Policy*, unless they have performed the following actions:

- Successfully perform public key operations as a condition of relying on a SWIFT Qualified Certificate.
- Validate a Certificate by using the SWIFTNet PKI CA's Certificate Revocation Lists (CRLs) (see also section 4.9.6).

- Untrust a SWIFT Qualified Certificate if it has been revoked or has expired.
- Take all other precautions with regard to the use of the SWIFT Qualified Certificate as set out in the present *Certificate Policy* or elsewhere, and rely on a SWIFT Qualified Certificate as may be reasonable under the circumstances.

4.6 Certificate Renewal

Certificate renewal as defined in PKI standards, that is, issuing a new Certificate to an existing key pair, is a functionality that is not implemented by the SWIFTNet PKI.

Subscribers who wish to renew their Certificates shall also be required to generate new key pairs (known as re-key).

4.7 Certificate Re-key

Re-Key requests are considered to be new Certificate requests. The same process applies as described in sections 4.1, 4.2, 4.3, and 4.4.

4.7.1 Circumstance for Certificate Re-key

When the private key corresponding to the SWIFT Qualified Certificate is less than 90 days away from expiring (“Valid To” date, as described in section 7.1), the Subscriber can submit a request for a new SWIFT Qualified Certificate, which will be validated, and either rejected or accepted and processed by SWIFTNet PKI RA.

Additionally, in case the Certificate has been revoked, the Subscriber can submit a request for a new SWIFT Qualified Certificate, which will be validated, and either rejected or accepted and processed by the SWIFTNet PKI RA.

4.7.2 Who May Request Certification of a New Public Key?

The same process as for initial Certificate application is used (section 4.1.1).

4.7.3 Processing Certificate Re-keying Requests

The same process as for initial Certificate application is used (section 4.2). As described in section 3.3, identity validation is repeated, which takes additional processing time.

4.7.4 Notification of New Certificate Issuance to Subscriber

The same process as for initial Certificate issuance is used (section 4.3).

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The same process as for initial Certificate acceptance is used (section 4.4.1).

4.7.6 Publication of the Re-keyed Certificate by the CA

The same process as for initial Certificate acceptance is used (section 4.4.2).

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The same process as for initial Certificate issuance is used (section 4.4.3).

4.8 Certificate Modification

Certificate modification is a functionality that is not implemented by the SWIFTNet PKI.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The Subscriber to which the SWIFT Qualified Certificate is issued must revoke the Certificate in case the associated private key is lost, in case the confidentiality of the private key is compromised, in case the information in the Certificate is no longer correct, and in case the confidentiality of the certificate generation activation secrets has been compromised or the certificate generation activation secrets are malfunctioning.

SWIFT as Certification Service Provider must revoke a SWIFT Qualified Certificate in exceptional circumstances as defined in the governing law: for example, in case SWIFT is informed of a strong suspicion that the registration information was wrong or falsified, of evidence that the information in the Certificate is no longer correct, that the confidentiality of the private key was compromised, or that the organisation to which the Certificate is issued (the Subscriber) stops existing.

SWIFT as Certification Service Provider must revoke all SWIFT Qualified Certificates in case of a court order, or in case it stops Certificate Service Provider activities without handing over to another CA with similar quality and security levels.

SWIFT as Certification Service Provider is also entitled to revoke SWIFT Qualified Certificates in the exceptional circumstance that any of the algorithms, or associated parameters, used by the CA or the Subscribers becomes insufficient for its remaining intended usage.

The revocation process is irreversible. Once revoked, the Certificate cannot be unrevoked.

4.9.2 Who Can Request Revocation?

The LSO account, as registered with SWIFT and entitled by the Subscriber to which it belongs to manage its SWIFT Qualified Certificates, uses the “Secure Channel” application to communicate with the SWIFTNet PKI RA, and to request a revocation for the SWIFT Qualified Certificate belonging to this Subscriber.

4.9.3 Procedure for Revocation Request

The LSO account, as registered with SWIFT and entitled by the Subscriber to which it belongs to manage its SWIFT Qualified Certificates, uses the “Secure Channel” application to communicate with the SWIFTNet PKI RA, and to request a revocation for the SWIFT Qualified Certificate belonging to this Subscriber.

4.9.4 Revocation Request Grace Period

There is no grace period, revocation is immediate.

The SWIFTNet PKI service does not enable the temporary suspension of Certificates.

The revocation process is irreversible. Once revoked, the Certificate cannot be unrevoked.

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation processing is performed by the SWIFTNet PKI RA, within 2 hours of reception of the revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are required to check revocation status of Certificates.

4.9.7 CRL Issuance Frequency

The CRL is issued immediately after a Certificate revocation.

If there is no revocation, then the CRLs are refreshed every 24 hours.

4.9.8 Maximum Latency for CRLs

The new CRL(s) will be added to the SWIFTNet Directory immediately following creation, and will be available for Relying Parties to download from the SWIFTNet Directory within 7 minutes after its creation.

The combined CRL available on https://www2.swift.com/pkirepository/SWIFTCA.crl is published every 24 hours.

4.9.9 Online Revocation/Status Checking Availability

Revocation status can be checked by consulting the CRL. CRLs are available to the Relying Parties on the SWIFTNet Directory, and on https://www2.swift.com/pkirepository/SWIFTCA.crl.

4.9.10 Online Revocation Checking Requirements

The SWIFTNet Link software is required to access the SWIFTNet Directory for accessing the CRLs. The combined CRL on https://www2.swift.com/pkirepository/SWIFTCA.crl is publicly available on the Internet.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements regarding Key Compromise

Not specified.

4.9.13 Certificate Suspension

Certificate suspension is a functionality that is not implemented by the SWIFTNet PKI.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Relying Parties are those persons who are acting on a SWIFT Qualified Certificate to verify the signature of a Subscriber.

Relying Parties that are SWIFT users can (re-)use their existing SWIFTNet connectivity to access the SWIFTNet Directory (see section 3.2.2). The SWIFTNet Link software is a mandatory component of this configuration, and is used to access the SWIFTNet Directory for accessing the CRLs.

Relying Parties that are not SWIFT users can access the combined CRL through the Internet on https://www2.swift.com/pkirepository/SWIFTCA.crl.

4.10.2 Service Availability

Resilience of the SWIFTNet systems is based on recovery scenarios that include fast service restoration if a disaster affects a SWIFT operating centre. The SWIFTNet systems are run at multiple operating centres located on geographically distributed locations. SWIFT has designed the operating centre environments to eliminate single points of failure. Each operating centre is designed to carry the whole of SWIFT's normal business with full local redundancy available.

SWIFT has designed all network connections between the operating centres to have at least two separate routes that can carry the full traffic load.

SWIFT organises planned maintenance, and business continuity testing, which occur during maintenance periods (known as allowable downtime windows). These maintenance windows and test windows begin on Saturday at 16:00 GMT. During the maintenance windows, the SWIFTNet PKI services are subject to possible interruptions.

The levels of service that this *Certificate Policy* specifies assume normal operating conditions. These include resilient operations during most single-component failure scenarios within the active and standby SWIFT operating centres. The SWIFTNet design is resilient, and can handle many anomalous events without impact to customer activities. However, under certain, very unlikely, disaster scenarios, SWIFT may be unable to meet these levels of service. The potential for data loss also exists in a few of these rare circumstances.

The availability of the repository that includes the combined CRL is designed to exceed 99.8% of SWIFTNet business hours - defined as 24 hours per day, seven days per week, excluding planned maintenance periods as indicated on www.swift.com > Support > Operational status.

4.11 End of Subscription

Subscription termination is governed by the appropriate clause in the relevant contractual arrangements in effect from time to time between the parties concerned directly.

When the subscription is terminated for reasons of breach of obligations, then SWIFT as Certification Service Provider will revoke the Subscriber’s SWIFT Qualified Certificate.

4.12 Key Escrow and Recovery

Key escrow is a functionality that is not implemented for SWIFT Qualified Certificates.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

Physical security controls are compliant with the SWIFT physical security policy, and are defined in the *SWIFT Qualified Certificates Certification Practice Statement* [1], according to the following themes:

- Site location and construction
- Physical access
- Power and air conditioning
- Water exposure
- Fire prevention and protection
- Media storage
- Waste disposal
- Off-site backup

5.2 Procedural Controls

Procedural security controls around the SWIFTNet PKI CA are defined in the *SWIFT Qualified Certificates Certification Practice Statement* [1] and related SWIFTNet PKI documentation. The following themes are included:

- Trusted roles
- Number of persons required per task
- Identification and authentication for each role
- Roles requiring separation of duties

5.3 Personnel Controls

Personnel security controls are compliant with the SWIFT HR Security policy. The following themes are included:

- Qualifications, experience, and clearance requirements
- Background check procedures
- Training requirements
- Retraining frequency and requirements
- Job rotation frequency and sequence
- Sanctions for unauthorised actions
- Independent contractor requirements
- Documentation supplied to personnel

5.4 Audit Logging Procedures

Audit logging procedures are defined in the *SWIFT Qualified Certificates Certification Practice Statement* [1], according to the following themes:

- Types of events recorded
- Frequency of processing log
- Retention period for audit log
- Protection of audit log
- Audit log backup procedures

5.5 Records Archival

Records archival is defined in the *SWIFT Qualified Certificates Certification Practice Statement* [1], according to the following themes:

- Types of records archived
- Retention period for archive

5.6 Key Changeover

Not applicable. SWIFTNet PKI Certificates will be issued with a validity time within the validity time of the CA root Certificate.

5.7 Compromise and Disaster Recovery

SWIFT maintains incident and crisis management procedures, and full Business Continuity Management processes. SWIFTNet PKI is part of these processes, and details are described in SWIFT internal documents.

5.8 CA or RA Termination

In case SWIFT decides to terminate its Qualified Certificate offering, the following procedures will be executed:

- When possible, transfer the Qualified Certificate service activities to a Certification Services Provider that can offer the same service levels as SWIFT.
- Inform Subscribers, Relying Parties, and the Belgian national supervisory body.
- Revoke all SWIFT Qualified Certificates 2 months after having notified the Subscribers.
- Maintain an archive of all events, Certificates, Certificate Status information, for as long as required.
- Decommission specific facilities and configuration for the SWIFTNet PKI CA to issue SWIFT Qualified Certificates.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is described in the *SWIFT Qualified Certificates Certification Practice Statement* [1], and is strictly organised and audited through PKI ceremonies.

Subscriber key pairs are generated inside an HSM, controlled by the KMA application.

6.1.2 Private Key Delivery to Subscriber

Not applicable: the private key is generated inside the HSM and is not exportable in clear text form.

6.1.3 Public Key Delivery to Certificate Issuer

The public key to be certified is sent in a KMA application request to the SWIFTNet PKI CA, inside a secure SWIFTNet session set up between Subscriber and SWIFT.

6.1.4 CA Public Key Delivery to Relying Parties

The SWIFTNet PKI CA public key is obtained automatically by the KMA application from the SWIFTNet PKI CA, inside a secure SWIFTNet session set up between Subscriber and SWIFT. Additionally, the SWIFTNet PKI CA public key certificate is available online on http://www.swift.com/pkirepository.

6.1.5 Key Sizes

The key size of the SWIFTNet PKI CA key pair, and all Entity Certificates, is 2048-bit RSA.

6.1.6 Public Key Parameter Generation and Quality Checking

All public key parameters are set by the SWIFTNet PKI RA. SWIFTNet PKI RA deploys procedures that implement quality control.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to section 7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The CA private key is generated and stored on a FIPS 140-1 or FIPS 140-2 level 3 HSM.

Subscriber private keys are generated and stored on an HSM that complies with minimally FIPS 140-1 or 140-2 level 2, provided by SWIFT (see section 1.3.5).

6.2.2 Private Key (n out of m) Multi-person Control

CA private key procedures are put in place to enforce that at least three representatives from different organisational units within SWIFT are required to perform security-critical functions.

Subscriber HSMs shall offer functionality that can be used by the Subscriber to implement Private Key Multi-person Control.

6.2.3 Private Key Escrow

No private key escrow functionality is implemented.

6.2.4 Private Key Back-up

There are no functions that allow the private key to be exported from the HSM, either in its entirety or in parts, in clear text form.

For the CA infrastructure, there is a special function that allows the HSM, including all keys and other data that is stored therein, to be securely "cloned". This is one of the security-critical functions noted in section 6.2.2 (and controlled as such).

For Subscriber HSMs, functionality shall not be available to allow private key back-up without assurance on access control, confidentiality, and traceability.

6.2.5 Private Key Archival

There are no functions that allow the private key to be exported from the HSM, either in its entirety or in parts, in clear text form.

6.2.6 Private Key Transfer into or from a Cryptographic Module

There are no functions that allow the private key to be exported from the HSM, either in its entirety or in parts, in clear text form.

For the CA private key, there is a special function that allows the HSM, including all keys and other data that is stored therein, to be securely "cloned". This is one of the security-critical functions noted in section 6.2.2 (and controlled as such).

For Subscriber HSMs, functionality shall not be available to allow private key transfer into or from a cryptographic module without assurance on access control, confidentiality, and traceability.

6.2.7 Private Key Storage on Cryptographic Module

The SWIFTNet PKI CA private signing key is stored in local HSMs that meet the FIPS140-1 or FIPS 140-2 level 3 standard.

Subscriber private keys are generated and stored on an HSM that complies with minimally FIPS 140-1 or 140-2 level 2, provided by SWIFT (see section 1.3.5).

6.2.8 Method of Activating Private Key

Not specified

6.2.9 Method of Deactivating Private Key

Not specified

6.2.10 Method of Destroying Private Key

There is a special function that allows the secure destruction of the information inside the HSM, including all keys and other data that is stored therein.

For the CA private key, this is one of the security-critical functions noted in section 6.2.2 (and controlled as such).

6.2.11 Cryptographic Module Rating

The SWIFTNet PKI CA uses an HSM that is compliant with FIPS 140-1 or FIPS 140-2 Level 3.

Subscribers use HSMs that comply with minimally FIPS 140-1 or 140-2 level 2.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Not specified.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Refer to section 7.1.

6.4 Activation Data

Activation data for the CA private key is handled as described in section 6.2.2.

Activation data for SWIFT Qualified Certificates are handled according to SWIFTNet security practices.

6.5 Computer Security Controls

Computer security controls are compliant with the SWIFT security policies.

6.6 Lifecycle Technical Controls

Lifecycle technical security controls are compliant with the SWIFT security policies.

6.7 Network Security Controls

Network security controls are compliant to the SWIFT security policies.

6.8 Time-stamping

Not specified.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Remark: The following fields of the Certificate format X.509 version 3 are not used in the SWIFTNet PKI:

- Issuer unique identifier
- Subject unique identifier

Field	Value	Detailed value *(or Example)*	Description/Comments
Version	*v3*	*2*	Corresponds to x509 v3
Serial Number		*45 a6 b6 32*	Serial number of Certificate in CA A unique Certificate serial number within the SWIFTNet PKI CA security domains, generated by the SWIFTNet PKI CA when a new Certificate is created
Signature algorithm	*sha256WithRSAEncryption*	*1.2.840.113549.1.1.11*	Identifier for the algorithm used by the SWIFTNet PKI CA to sign the Certificate
Issuer	*o=swift*		The full distinguished name of the SWIFTNet PKI CA issuing the Certificate
Valid from		*Mar 25 15:57:58 2012 GMT*	Certificate validity period: maximum 2 years for SWIFT Qualified Certificates. The “valid to” date is set by SWIFTNet PKI RA as 2 years after the date of defining the Certificate parameters (see section 4.1.2). The “valid from” date is set by the SWIFTNet PKI CA as the date of Certificate generation (see section 4.3). The Certificate generation takes place maximum 180 days after the certificate generation activation secrets are issued.
Valid to		*Mar 25 16:27:58 2014 GMT*	

Field	Value	Detailed value *(or Example)*	Description/Comments
Subject	*cn=%<number>,cn=Qualified Enterprise,o=<BIC>,o=swift* or *cn=Qualified Enterprise, o=<BIC>,o=swift*	*cn=%001,cn=Qualified Enterprise, o=bankbebb,o=swift* *cn=Qualified Enterprise, o=bankbebb,o=swift*	*<number>* is a numeric string with a maximum length of 8 digits (each with value 0 to 9). The *cn=%<number>* part is optional. *<BIC>* is an identifier for the Certificate Subscriber identity, the ISO-9362 Business Identifier Code
Public key	RSA public key, 2048 bit Modulus = 2048 bit, Public Exponent = 65537		
Extensions	See table below		

Remark: The following extensions are not used in the SWIFTNet PKI:

- Policy Constraints
- Policy Qualifiers. SWIFT Qualified Certificates don't contain a URI (Uniform Resource Identifier) to the Certification Practice Statement document, or a UserNotice.

Extension name	Extension OID	Value	Detailed value *(or Example)*	Critical	Description/ Comments
KeyUsage	2.5.29.15	Digital signature, Non-Repudiation		True	
IssuerAltName	2.5.29.18	*CN=SWIFTNet PKI CA, O=S.W.I.F.T. SCRL, C=BE*		False	Indicates the name of the organisation as stated in the official records, and the country in which it is established.
SubjectDirectory Attributes	2.5.29.9			False	Pointer to the attribute Certificate describing the password policies defined on the CA.
CertificatePolicies	2.5.29.32	*1.3.21.6.3.10.200.3*		False	SWIFT Qualified Certificate.
qcStatements	1.3.6.1.5.5.7.1.3	id-etsi-qcs 1	0.4.0.1862.1.1	False	ETSI TS 101862

Extension name	Extension OID	Value	Detailed value *(or Example)*	Critical	Description/ Comments
CRLDistributionPoints	2.5.29.31	*DirName:/O=SWIFT/CN=CRLnnn*	*cn=CRL167,o=swift*	False	Distinguished Name (DN) where the revocation information about the Certificate will be published in the SWIFTNet Directory. The combined CRL is additionally available on https://www2.swift.com/pkirepository/SWIFTCA.crl.
PrivateKeyUsagePeriod	2.5.29.16	NotBefore, NotAfter have same values as “Valid from” and “Valid to”		False	Private Key is valid for 100% of the corresponding Certificate lifetime.
AuthorityKeyIdentifier	2.5.29.35	160-bit key identifier		False	Helps identify the correct CA public key. It is typically a SHA1 digest of the CA public key.
SubjectKeyIdentifier	2.5.29.14	160-bit key identifier		False	Helps identify the correct subject public key. It is typically a SHA1 digest of the public key.
BasicConstraints	2.5.29.19	*CA = False*		False	Indicates whether Subject is a CA or not.
EntrustVersInfo	1.2.840.113533.7.65.0			False	Indicates Entrust version.

7.2 CRL Profile

7.2.1 Partitioned CRL

The following fields of the X.509 version 2 CRL format are used in the SWIFTNet PKI.

Field	Value	Detailed value *(or Example)*	Description/Comments
Version	*v2*	*1*	Corresponds to x509 v2 CRL profile.
Signature algorithm	*sha1WithRSAEncryption*	*1.2.840.113549.1.1.1*	Identifier for the algorithm used by the SWIFTNet PKI CA to sign the CRL.
Issuer	*o=swift*		The full distinguished name of the SWIFTNet PKI CA

Field	Value	Detailed value *(or Example)*	Description/Comments
			issuing the CRL.
Last (This) Update		*May 11 15:57:58 2012 GMT*	Issue date of this CRL.
Next Update		*May 12 16:57:58 2012 GMT*	Next CRL update will be issued no later than the indicated date.
Revoked Certificates			If present, it is a non-empty list of revoked Certificates. Each element in the list is also known as a CRL-entry.
Serial Number		*4B 04 53 AF*	Certificate serial number.
Revocation Date		*Mar 22 17:59:09 2012 GMT*	Revocation date and time.
Extensions	See table below		

CRLs issued by the SWIFTNet PKI CA are X.509 version 2 CRLs.

A number of X.509 version 2 CRL and CRL entry extensions are used in the SWIFTNet PKI. These are outlined below. The X.509 version 2 CRL and CRL entry extensions that are never present in CRLs issued by the SWIFTNet PKI CA, are also outlined below.

The following CRL and CRL entry extensions are used in this PKI.

CRL Extension name	Value	Detailed value *(or Example)*	Critical	Description/ Comments
IssuingDistribution Point		*CN=CRL624, O=SWIFT*	True	Identifies the CRL distribution point.
CRL Number			False	Monotonically increasing sequence number for a given CRL scope and CRL issuer.
AuthorityKeyIdentifier	160-bit key identifier		False	Identifies the public key corresponding to the private key used to sign the CRL. It is typically a SHA1 digest of the public key.
Issuer alternative name				Not used.
Delta CRL indicator				Not used.
Delta CRL Distribution Point (Freshest CRL)				Not used.

CRL Entry Extension name	Value	Detailed value *(or Example)*	Critical	Description/ Comments
CRL Reason Code		For example Key Compromise	False	Reason for the Certificate revocation.

Invalidity Date		*Mar 22 17:59:09 2012 GMT*	False	The date on which it is known or suspected that the private key was compromised or that the Certificate otherwise became invalid. For SWIFTNet PKI, this is identical to the Revocation date and time.
Hold instruction code				Not used.
Certificate issuer				Not used.

7.2.2 Combined CRL

The following fields of the X.509 version 2 CRL format are used in the SWIFTNet PKI.

Field	Value	Detailed value *(or Example)*	Description/Comments
Version	*v2*	*1*	Corresponds to x509 v2 CRL profile.
Signature algorithm	*sha1WithRSAEncryption*	*1.2.840.113549.1.1.1*	Identifier for the algorithm used by the SWIFTNet PKI CA to sign the CRL.
Issuer	*o=swift*		The full distinguished name of the SWIFTNet PKI CA issuing the CRL.
Last (This) Update		*May 11 15:57:58 2012 GMT*	Issue date of this CRL.
Next Update		*May 14 15:57:58 2012 GMT*	Next CRL update will be issued no later than the indicated date.
Revoked Certificates			If present, it is a non-empty list of revoked Certificates. Each element in the list is also known as a CRL-entry.
Serial Number		*4B 04 53 AF*	Certificate serial number.
Revocation Date		*Mar 22 17:59:09 2012 GMT*	Revocation date and time.
Extensions	See table below		

CRLs issued by the SWIFTNet PKI CA are X.509 version 2 CRLs.

A number of X.509 version 2 CRL and CRL entry extensions are used in the SWIFTNet PKI. These are outlined below. The X.509 version 2 CRL and CRL entry extensions that are never present in CRLs issued by the SWIFTNet PKI CA, are also outlined below.

The following CRL and CRL entry extensions are used in this PKI.

CRL Extension name	Value	Detailed value *(or Example)*	Critical	Description/ Comments
CRL Number			False	Monotonically increasing sequence number for a given CRL scope and CRL issuer.
AuthorityKeyIdentifier	160-bit key identifier		False	Identifies the public key corresponding to the private key used to sign the CRL. It is typically a SHA1 digest of the public key.
IssuingDistribution Point				Not used.
Issuer alternative name				Not used.
Delta CRL indicator				Not used.
Delta CRL Distribution Point (Freshest CRL)				Not used.

CRL Entry Extension name	Value	Detailed value *(or Example)*	Critical	Description/ Comments
CRL Reason Code		For example Key Compromise	False	Reason for the Certificate revocation.
Invalidity Date		*Mar 22 17:59:09 2012 GMT*	False	The date on which it is known or suspected that the private key was compromised or that the Certificate otherwise became invalid. For SWIFTNet PKI, this is identical to the Revocation date and time.
Hold instruction code				Not used.
Certificate issuer				Not used.

7.3 OCSP Profile

Not applicable.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Complementing the mandatory supervision audits, as part of the Belgian national supervisory body's processes, SWIFT has appointed its Internal Audit team as the independent auditor who will review compliance with the requirements as laid out in this *Certificate Policy*.

8.1 Frequency or Circumstances of Assessment

Under its current mandate, Internal Audit operates on a three-year cycle. This means that an audit entity will be audited at least once every three years, or more frequently depending on the business criticality as defined by Internal Audit and SWIFT Management. The business criticality is reconfirmed at the start of every assessment.

SWIFT Management can always request a specific review in addition to the normal rotational coverage described above.

The Certificate lifecycle processes, as well as the physical and logical security measures protecting the Certification Authority (CA) and related systems, are generic for all Certificates produced by SWIFT, which are part of SWIFT's annual ISAE 3402 report which includes the opinion of the external security auditor on the adequacy and effectiveness of the controls.

8.2 Identity and Qualifications of Assessor

Notwithstanding the appointment of an independent external assessor in the context of the mandatory supervision audits (as part of the Belgian national supervisory body's processes), SWIFT's Internal Audit team has been appointed as independent auditor. The team has multiple technology experts that have adequate skills to perform the assessment. As a baseline, all technology experts have the professional accreditation awarded by ISACA – Certified IT Systems Auditor (CISA) and many have additional professional accreditations such as ISC2's Certified Information Systems Security Professional (CISSP).

The Chief Auditor can elect to assign this work partly or entirely to a third party. In this case, the third party will have similar or better qualifications and the report will still be issued under the responsibility of the Chief Auditor. All other stipulations in this section will continue to apply.

8.3 Assessor's Relationship to Assessed Entity

The Internal Audit team is independent from SWIFT's Management and the Chief Auditor has a direct reporting line to the Chairman of SWIFT's Audit & Finance Committee (as well as to SWIFT's Chief Executive Officer). The Internal Audit Charter provides for numerous safeguards that ensure continued independence for the Internal Audit team.

8.4 Topics Covered by Assessment

The topics covered in each assessment can change from review to review, but as a minimum will include a complete effectiveness review of all controls included in this document.

8.5 Actions Taken as a Result of Deficiency

Issues and findings resulting from the assessment are reported to Management. The final audit report includes the issues and findings as well as the agreed corrective action plan and target date for resolution. The issues and findings are tracked until resolution by Internal Audit.

8.6 Communication of Results

The report of the assessment is for SWIFT Management only and is not disclosed to third parties unless in support of the mandatory supervision audits as part of the Belgian national supervisory body's processes, or other SWIFT assurance efforts for which the work performed is relevant (any other exceptions to this distribution policy will have to be approved by the Chief Auditor). The Certificate lifecycle processes, as well as the physical and logical security measures protecting the Certification Authority (CA) and related systems, are generic for all Certificates produced by SWIFT, these are part of SWIFT's annual ISAE 3402 report which includes the opinion of the external security auditor on the adequacy and effectiveness of the controls. The ISAE 3402 report is available to all registered users of SWIFT.

9 OTHER BUSINESS AND LEGAL MATTERS

The *SWIFT Qualified Certificates Terms and Conditions* constitute the main set of SWIFT standard terms and conditions for the provision and use of SWIFT's Qualified Certificates offering. For example, they provide general information about the conditions of use of SWIFT Qualified Certificates, the rights and obligations of SWIFT, the Subscribers and Relying Parties, including the duration and termination conditions, their liability, the claim process, or the applicable law and jurisdiction.

If and to the extent that SWIFT's Qualified Certificates offering is used in conjunction with other SWIFT services and products, the *SWIFT Qualified Certificates Terms and Conditions* must be read together with the terms and conditions governing the provision and use of these other SWIFT services and products.

The *SWIFT Qualified Certificates Terms and Conditions* apply each time the form or contract executed by the Subscriber or Relying Party (i) refers to the provision and use of SWIFT Qualified Certificates and (ii) expressly confirms that these SWIFT Qualified Certificates Terms and Conditions apply. If the Relying Party has not executed any such form or contract, it shall be deemed to have tacitly accepted the *SWIFT Qualified Certificates Terms and Conditions* by relying or other acting upon a SWIFT Qualified Certificate.

The form or contract (if any) executed by the Subscriber or Relying Party and the *SWIFT Qualified Certificates Terms and Conditions*, together with this *Certificate Policy* and the *SWIFT Qualified Certificates Certification Practice Statement* ("CPS") which are incorporated in the Qualified Certificate Terms and Conditions by reference, constitute the agreement between SWIFT and the Subscriber or Relying Party for the provision and use of SWIFT Qualified Certificates (the "Qualified Certificates Agreement").

The sections below provide useful information about certain terms and conditions governing the provision or use of SWIFT's Qualified Certificates offering, as may be set out in more detail elsewhere in the Qualified Certificates Agreement. Nothing in these sections shall be interpreted or construed as granting any rights or imposing any obligations in addition to those set out in the *SWIFT Qualified Certificates Terms and Conditions*.

9.1 Fees

The Subscriber and Relying Party must pay to SWIFT all charges and fees (if any) applicable to it for the provision or use of SWIFT's Qualified Certificates offering.

These charges and fees, and related invoicing and payment terms and conditions, are as notified by SWIFT from time to time.

For more information, see clause 7 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.2 Financial Responsibility

SWIFT shall monitor on a regular basis that it maintains adequate resources and insurance coverage to meet its obligations regarding the provision and use of its Qualified Certificate offering under this *Certificate Policy* and elsewhere in the Qualified Certificates Agreement.

9.3 Confidentiality of Business Information

The obligations of confidence of SWIFT, Subscribers and Relying Parties in respect of confidential information obtained in connection with the provision or use of SWIFT's Qualified Certificates offering are as set out in this *Certificate Policy* and elsewhere in the Qualified Certificates Agreement.

Examples of confidential business information include:

- the Subscriber's confidential information supplied to SWIFT at the time of its subscription (other than any information that is published in a SWIFT Qualified Certificate)
- the Subscriber's or Relying Parties' confidential information supplied to SWIFT in support requests (other than any information that is published in a SWIFT Qualified Certificate)
- the private key(s) of SWIFT Qualified Certificates

For the avoidance of any doubt, the following information is not considered as confidential:

- the information published in a SWIFT Qualified Certificate
- the revocation records of a SWIFT Qualified Certificate
- this *Certificate Policy*

For more information, see clause 11 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.4 Privacy of Business Information

SWIFT may process personal data (as defined in the *SWIFT Personal Data Protection Policy*) collected:

a) by SWIFT for purposes relating to the provision of SWIFT services and products, including SWIFT's Qualified Certificates offering, or relating to SWIFT governance (for example, contact details of or secrets used to authenticate employees, security officers, or other representatives of a Subscriber or Relying Party)
b) by a Subscriber or Relying Party and supplied to SWIFT as part of the Subscriber's or Relying Party's use of SWIFT's Qualified Certificates offering (for example, personal data contained in Certificates that the Subscriber requests SWIFT to issue).

The rights and obligations of all parties concerned in each case are set out in the SWIFT Personal Data Protection Policy [2] in effect from time to time as published on www.swift.com.

For more information, see clause 10 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.5 Intellectual Property Rights

Any and all rights (including title, ownership rights, database rights, and any other intellectual property rights) in SWIFT's Qualified Certificates offering, and documentation or other materials developed or supplied in connection with that offering, including any associated processes or any derivative works, are and will remain the sole and exclusive property of SWIFT or its licensors.

No rights are granted by SWIFT in respect of SWIFT's Qualified Certificates offering other than those expressly granted under this *Certificate Policy* or elsewhere in the Qualified Certificates Agreement.

For more information, see clause 6 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.6 Representations and Warranties

SWIFT is responsible for the provision of its Qualified Certificates offering, as set out in this *Certificate Policy* and elsewhere in the Qualified Certificates Agreement.

The Subscribers are responsible for complying with all obligations and other responsibilities applicable to their use of SWIFT's Qualified Certificates offering as set out in this *Certificate Policy* and elsewhere in the Qualified Certificates Agreement.

Examples of Subscribers' obligations and responsibilities include (without limitation):

- the protecting of the private key(s) related to their SWIFT Qualified Certificate
- the protection of the HSM in which the private key of their SWIFT Qualified Certificates is stored
- the protection of the Activation Data of their SWIFT Qualified Certificates
- the protection of the certificate generation activation secrets of their SWIFT Qualified Certificates
- the immediate revocation of their SWIFT Qualified Certificate if the associated private key is lost, the confidentiality of the private key is compromised, the information in the Certificate is no longer correct, or if the confidentiality of the certificate generation activation secrets has been compromised or the certificate generation activation secrets are malfunctioning (for more information, see also section 4.9.1)

The Relying Parties are responsible for complying with their obligations and other responsibilities applicable to their use of SWIFT's Qualified Certificates offering as set out in this *Certificate Policy* and elsewhere in the Qualified Certificates Agreement.

Examples of Relying Parties' obligations and responsibilities include (without limitation):

- the successful performance of public key operations as a pre-condition for relying on a SWIFT Qualified Certificate
- the validation of a SWIFT Qualified Certificate by using the SWIFTNet PKI CA's Certificate Revocation Lists (CRLs)
- the immediate termination of any reliance on a SWIFT Qualified Certificate if it has been revoked or when it has expired

9.7 Disclaimers of Warranties

To the maximum extent permitted by applicable law and except as expressly provided in this *Certificate Policy* or elsewhere in the Qualified Certificates Agreement, SWIFT does not give and specifically excludes and disclaims any warranty of any kind, whether express or implied, statutory or otherwise, with respect to the provision or use of SWIFT's Qualified Certificates offering, including (without limitation) any warranty as to the condition, quality, performance, non-infringement, merchantability or fitness for a particular purpose.

For more information, see clause 8 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.8 Limitation of Liability

SWIFT's liability to Subscribers or Relying Parties (whether in contract, tort, or otherwise) for or in connection with the provision for use of SWIFT's Qualified Certificates offering, including any limitations or exclusions of liability, are set out in the *SWIFT Qualified Certificates Terms and Conditions*.

For more information, see clause 8 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.9 Indemnities

Indemnities (if any) applicable to SWIFT, Subscribers or Relying Parties are set out the *SWIFT Qualified Certificates Terms and Conditions*.

For more information, see clause 8 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.10 Term and Termination

This *Certificate Policy* shall be effective from the date of issue and publication, and will remain in force until replaced with a subsequent version, or terminated.

For more information about the term and termination of SWIFT's Qualified Certificate Offering, see clause 9 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.11 Individual Notices and Communications with Participants

Except when expressly provided otherwise in the Qualified Certificates Agreement, all notices from one party to another, will be in writing (in paper or electronic form) and in English.

All notices duly served will be deemed effective upon their receipt by the recipient.

For more information, see clause 12 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.12 Amendments

This *Certificate Policy* shall be reviewed on a regular basis as set out in section 1.5.4. Like for the other documents that are part of the Qualified Certificates Agreement, it can be amended at any time by publishing a new version.

Consequently, the Subscribers and Relying Parties must ensure that they always refer to the latest version of this *Certificate Policy* and any other documents part of the Qualified Certificates Agreement, and that they are aware of the latest available information relating to the provision and use of SWIFT's Qualified Certificates offering.

Proposed changes to the present *Certificate Policy* or other documents part of the Qualified Certificates Agreement will be disseminated to interested parties by publishing the new document on http://www.swift.com/pkirepository.

The date of publication and the effective date are indicated on the title page of the relevant document. The effective date will at least be fourteen (14) calendar days after the date of publication.

9.13 Dispute Resolution Procedures

To make a valid claim in connection with the provision or use of SWIFT's Qualified Certificates offering, Subscribers and Relying Parties must submit their claim to SWIFT in accordance with the dispute resolution procedure set out in the *SWIFT Qualified Certificates Terms and Conditions*.

For more information, see clause 9.13 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.14 Governing Law

As per clause 9.14 of the *SWIFT Qualified Certificates Terms and Conditions,* this *Certificate Policy* and, more generally, the Qualified Certificates Agreement are governed by and construed in accordance with Belgian law (without giving effect to any conflict of law provision that would cause the application of other laws).

9.15 Compliance with Applicable Law

In using SWIFT's Qualified Certificates offering, Subscribers and Relying Parties must always exercise due diligence and reasonable judgment, and must comply with good industry practice and all relevant laws, regulations, or third-party rights, even if this restricts their usage of SWIFT's Qualified Certificates offering.

In particular, Subscribers and Relying Parties must seek all necessary or advisable consents and authorisations and enter into all necessary contractual arrangements in order to ensure that no laws, regulations, or third-party rights are violated (including laws and regulations regarding banking, money transmission, securities, money laundering, terrorist financing, economic sanctions, competition, outsourcing and data transmission).

Subscribers and Relying Parties must also comply with all relevant laws and regulations regarding the export, re-export, import, and use of any products, software, technology, or materials (including cryptographic technology and materials) comprised in or relating to the provision and the use of SWIFT's Qualified Certificates offering.

For more information, see clause 5.2 of the *SWIFT Qualified Certificates Terms and Conditions*.

9.16 Miscellaneous Provisions

No stipulation.

Annex – SWIFT Qualified Certificate Lifecycle Overview

The lifecycle of a SWIFT Qualified Certificate starts with an organisation identifying the need for such a Certificate. Refer to the description of Subscriber in section 1.3.3, that is, "Subscribers of SWIFT Qualified Certificates are those organisations that contract with SWIFT for the issuance of a SWIFT Qualified Certificate in their name. Typically, Subscribers are SWIFT users that require a SWIFT Qualified Certificate to sign messages or files sent over the SWIFT network."

Prerequisite

The subscribing organisation takes the steps required to join SWIFT (if not already the case), and to contract with SWIFT for a service requiring a SWIFT Qualified Certificate. As part of joining SWIFT,

- The subscribing organisation will acquire SWIFT Secure IP Network (SIPN) connectivity, SWIFTNet Link (SNL) software used to communicate with SWIFTNet over SIPN, and a Hardware Security Module (HSM) for handling the cryptographic material.
- The subscribing organisation will define at least two LSO accounts that obtain an account on the Secure Channel service, protected with a userid, a password, and a secure code card. Note: The Subscriber can also define if these LSO accounts need dual authorisation for their activities.

Registration

As part of the ordering and contracting process,

- SWIFT will perform an identity verification process, referred to as "QC Customer Identification". This process is the Subscriber registration phase, and will provide assurance on the identity of the Subscriber and a natural person representing it. When this QC Customer Identification process has been performed, the Subscriber is informed of this, and of the status of the outcome (success or failure). Only if the outcome is successful, the subscribing organisation is eligible to obtain a SWIFT Qualified Certificate. In this case, SWIFT provides the Subscriber with user documentation on how to request SWIFT Qualified Certificates.
- The Subscriber must appoint at least two LSO accounts (from the ones the organisation created at that point, as a result of its SWIFT network connectivity setup) that are henceforth formally mandated to manage the Subscriber's SWIFT Qualified Certificate.
  This list of mandated LSO accounts is reconfirmed at every subsequent QC Customer Identification.

If the outcome of the QC Customer Identification process is successful, then the Subscriber (via one of the mandated LSO accounts) can formally request a SWIFT Qualified Certificate.

Certificate Application

A mandated LSO account sends a SWIFT Qualified Certificate request through the Secure Channel application. This request is authenticated with the secure code card, and approved by a second LSO account if the dual authorisation functionality was enabled by the Subscriber.

As part of the request, the LSO account specifies a "download password".

Certificate Application Validation by RA

As result of this Secure Channel request, the SWIFTNet PKI RA will validate the request, and if all validations are positive, the requested certificate will be created.

An important validation step is that the QC Customer Identification process must have been completed successfully with a validation date no longer than 3 months before the Secure Channel request. In case it is not recent enough, the QC Customer Identification process has to be executed first. The certificate creation consists of putting the related Subject DN (together with all other certificate parameters – except the public key and "valid from" date) in the PKI system

as “ready for certification”, which results in issuing “certificate generation activation secrets”. These “certificate generation activation secrets” are made available for download by the LSO account using the password defined as part of the request, and an email is sent to this account (and the authorising account) as acknowledgement.

Certificate Request

The LSO account uses a computer connected to SIPN to navigate to the download page, specifies the “download password”, and receives the “certificate generation activation secrets”. This can be performed only once. The “certificate generation activation secrets” remain valid for 180 days.

> Note: At this point, if the Subscriber decides that there is no longer a need for the SWIFT Qualified Certificate, then he can decide to deactivate the “certificate generation activation secrets” by means of the Secure Channel application.

The LSO account transmits these “certificate generation activation secrets” to an operator of the SNL software (it can be the same person, but typically these are different roles in the organisation). The operator launches the SNL “KMA” application to generate the key pair on the HSM, to specify a password for accessing the private key (“activation data”), and to send the public key together with the “certificate generation activation secrets” to the SWIFTNet PKI CA (transported over SIPN[3]).

Certification

The SWIFT Qualified Certificate is generated based on the public key, the Subject DN, and other certificate parameters as defined by the SWIFTNet PKI RA. The generated SWIFT Qualified Certificate is returned to the KMA application.

Certificate Acceptance

The SWIFT Qualified Certificate is installed by the KMA application alongside the key pair.

KMA receives from the CA some policy statements as defined by the SWIFTNet PKI RA, requiring the key pair to be generated on HSM, and the password policy to be enforced for the “activation data”. The KMA software enforces these policy statements for the operator.

Renew (Re-key) Certificate

In case the old SWIFT Qualified Certificate is expired, revoked, or about to expire, a process enables the Subscriber to obtain a new one. The state “about to expire” is defined as the time-period 90 days before the certificate will expire.

The process to obtain a new SWIFT Qualified Certificate consists of the same steps as described above for the initial Certificate request:

- Certificate Application
- Certificate Application Validation by RA
  Note: this includes the validation of the required conditions for a new certificate request.
- Certificate Request
- Certification
- Certificate Acceptance

Revoke Certificate

At any time, the Subscriber can revoke its SWIFT Qualified Certificate, for example, if there is suspicion that the private key is compromised or stolen, or if the private key is lost or deleted. To perform such a revocation, the Subscriber (through one of the mandated LSO accounts) uses the Secure Channel application to request the revocation of its SWIFT Qualified Certificate. This request is authenticated with the secure code card, and approved by a second LSO account if the dual authorisation functionality was enabled by the Subscriber.

[3] Using the PKIX-CMP protocol

As result of this Secure Channel request, the SWIFTNet PKI RA will validate the request, and if all validations are positive, it will revoke the certificate. The CRL will be updated and published automatically. After revocation, the LSO account (and, if relevant, the authorising account) receives a confirmation.

References

The following referenced documents bring additional detailed information to this *Certificate Policy*.

[1] *SWIFT Qualified Certificates Certification Practice Statement*

[2] *SWIFT Personal Data Protection Policy*

[3] *SWIFT Qualified Certificates Certificate Administration Guide*

Legal Notices

Copyright

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

Translations

The English version of SWIFT documentation is the only official and binding version.

Trademarks