SWIFT

SWIFT Qualified Certificates for Electronic Seals

PKI Disclosure Statement

This *PKI Disclosure Statement* applies to SWIFT Qualified Certificates for Electronic Seals issued by SWIFT. It supplements the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy* and *SWIFT Qualified Certificates for Electronic Seals – Certification Practice Statement* by summarising their key points for the benefit of subscribers and relying parties. This document is effective from 3 November 2017.

20 October 2017

Table of Contents

Preface

Purpose of this document

This *PKI Disclosure Statement* is for use as a supplemental instrument of disclosure and notice by SWIFT. This *PKI Disclosure Statement* (PDS) assists SWIFT to respond to regulatory requirements and concerns, particularly those related to consumer deployment.

Although *Certificate Policy* (CP) and *Certification Practice Statement* (CPS) documents are essential for describing and governing certificate policies and practices, many PKI users, especially consumers, find these documents difficult to understand. Consequently, there is a need for a supplemental and simplified instrument that can assist PKI users in making informed trust decisions. This *PKI Disclosure Statement* is not intended to replace a CP or CPS, and nothing herein shall be interpreted or construed as granting any rights or imposing any obligations in addition to those set out in a CP or CPS.

This *PKI Disclosure Statement* applies to SWIFT Qualified Certificates for Electronic Seals issued by SWIFT.

1 Introduction

This *PKI Disclosure Statement* is intended to provide PKI participants (subscribers and relying parties) with a short extract of SWIFT Qualified Certificates for Electronic Seals PKI policy documentation which focuses on key information of interest to users.

This PDS is based on the format defined in annex A of ETSI EN 319411-1.

2 Policy Authority & Issuing Authority Contact Info

2.1 Policy Authority

SWIFT SCRL – IT – Global Security
Avenue Adele 1
1310 La Hulpe
Belgium

Tel: +32 2 655 41 24 - E-mail: swift-pma@swift.com

RPM Nivelles – VAT BE 0413330856

2.2 Issuing Authority

SWIFT SCRL – IT – Global Security
Avenue Adele 1
1310 La Hulpe
Belgium

Tel: +32 2 655 41 24 - E-mail: swift-pma@swift.com

RPM Nivelles – VAT BE 0413330856

3 Certificate Type, Validation Procedures and Usage

The Certificates issued under the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy* provide assurance of the identity of the Subscriber, and are for use in conjunction with specific SWIFT services and products allowing use of such Qualified Certificates for Electronic Seals as documented in the relevant service documentation.

The identity validation process includes the verification by SWIFT of the identity of the Subscriber and involves in-person identity verification of its authorised representative(s). 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 12 years as from the expiry or revocation date of the certificate (whichever occurs first).

The permitted usage of a SWIFT Qualified Certificate for Electronic Seals is limited to the support of advanced electronic seals in connection with the provision and use of specific SWIFT services and products only.

4 Reliance Limits

Qualified Certificates for Electronic Seals may not be used for any purpose other than advanced electronic seals as defined in the eIDAS Regulation[1] and as further set forth in the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy*.

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 for Electronic Seals offering, including any limitations or exclusions of liability, are set out in the *SWIFT Qualified Certificates for Electronic Seals – Terms and Conditions*.

5 Obligations of Subscribers

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

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

- the protection of the private key(s) related to their SWIFT Qualified Certificate for Electronic Seals
- the protection of the HSM in which the private key of their SWIFT Qualified Certificates for Electronic Seals is stored
- the protection of the Activation Data of their SWIFT Qualified Certificates for Electronic Seals
- the protection of the certificate generation activation secrets of their SWIFT Qualified Certificates for Electronic Seals
- the immediate revocation of their SWIFT Qualified Certificate for Electronic Seals if any of the following circumstances occurs:
    - the associated private key is lost;
    - the Subscriber has reasons to believe the confidentiality of the private key has been compromised;
    - the information in the certificate is no longer correct;
    - the confidentiality of the certificate generation activation secrets has been compromised or the certificate generation activation secrets are malfunctioning.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.

6 Certificate Status Checking Obligations of Relying Parties

The Relying Parties are responsible for complying with their obligations and other responsibilities applicable to their use of SWIFT's Qualified Certificates for Electronic Seals offering as set out in the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy* and elsewhere in the Qualified Certificates for Electronic Seals 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 for Electronic Seals
- the validation of a SWIFT Qualified Certificate for Electronic Seals by using the SWIFTNet PKI CA's Certificate Revocation Lists (CRLs)
- untrust a SWIFT Qualified Certificate for Electronic Seals once it has been revoked or has expired

7 Limited Warranty & Disclaimer/Limitation of Liability

The *SWIFT Qualified Certificates for Electronic Seals – Terms and Conditions* contain the provisions governing 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 for Electronic Seals offering, including any limitations or exclusions of SWIFT's liability

To the maximum extent permitted by applicable law and except as expressly provided in the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy* or elsewhere in the Qualified Certificates for Electronic Seals Agreement or other applicable contractual arrangements between SWIFT and the Subscriber or the Relying Party, 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 for Electronic Seals offering, including (without limitation) any warranty as to the condition, quality, performance, security, non-infringement, merchantability or fitness for a particular purpose.

For more information, see in particular clause 8 of the *SWIFT Qualified Certificates for Electronic Seals – Terms and Conditions*.

8 Applicable Agreements, CPS, CP

SWIFT documentation including the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy, SWIFT Qualified Certificates for Electronic Seals – Certification Practice Statement* and *SWIFT Qualified Certificates for Electronic Seals – Terms and Conditions are available at:*

https://www.swift.com/pkirepository

9 Privacy Policy

SWIFT processes 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 for Electronic Seals offering, or relating to SWIFT governance or other purposes set out in the *SWIFT Personal Data Protection Policy* (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 for Electronic Seals offering

(for example, personal data contained in certificates that the Subscriber requested SWIFT to issue).

The rights and obligations of all parties concerned in each case are set out in the SWIFT Personal Data Protection Policy in effect from time to time as published on www.swift.com, such as any notification obligation SWIFT may have in case of unauthorised disclosure of personal data supplied by the Subscriber or Relying Party.

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

10 Refund Policy

The Subscriber and/or Relying Party must pay to SWIFT all charges and fees (if any) applicable to them for the provision or use of SWIFT's Qualified Certificates for Electronic Seals 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 for Electronic – Terms and Conditions*.

11 Applicable Law, Complaints and Dispute Resolution

As per clause 15 of the *SWIFT Qualified Certificates for Electronic Seals – Terms and Conditions,* the *SWIFT Qualified Certificates for Electronic Seals – Certificate Policy* and, more generally, the Qualified Certificates for Electronic Seals Agreement and all contractual and non-contractual obligations arising out of them or in connection with them shall be 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).

To make a valid claim, Subscribers and Relying Parties must submit their claim to SWIFT in accordance with the dispute resolution procedure set out in clause 14 of the *SWIFT Qualified Certificates for Electronic Seals – Terms and Conditions*.

12 TSP and Repository Licenses, Trust Marks, and Audit

SWIFT is listed on the Belgian Trusted List: https://tsl.belgium.be/tsl-be.xml

Legal Notices

S.W.I.F.T. SCRL (“SWIFT”), Avenue Adèle 1, 1310 La Hulpe,

Belgium. RPM Nivelles – VAT BE 0413330856

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