Preface
This document gives an overview of the functions and technical features of the SWIFTNet Public Key Infrastructure (PKI) Service.

SWIFTNet PKI is the mandatory soft-and hardware needed to secure the SWIFTNet Services. It is installed alongside SWIFTNet Link.

This document should be read by:
- SWIFT users wishing to take advantage of this product requiring more detailed technical information.
- User and vendor application development and support personnel who need general information about the features of SWIFTNet PKI.

It contains the following information:
- An overview of the uses and benefits of SWIFTNet PKI (the value for the customer)
- A description of the key features and functions of SWIFTNet PKI
- Operational requirements
- An overview of the additional support services
- A glossary of abbreviations and terms

Note: This overview might contain advance information that is subject to change and evolution.
Table of contents

1 An Introduction to SWIFTNet PKI ................................................................. 1

2 Value for Customer .......................................................................................... 2
  2.1 General ........................................................................................................... 2
  2.2 Trust .............................................................................................................. 2
  2.3 Guarantees .................................................................................................. 2
  2.4 A Strong PKI ............................................................................................... 3

3 Features and Functions .................................................................................... 5
  3.1 PKI Client Components ............................................................................... 5
  3.1.1 Local Registration Application ............................................................... 5
  3.1.2 Cryptographic and Certificate Management APIs .................................. 5
  3.2 PKI SWIFT Components ........................................................................... 6
  3.2.1 Registration Authority ............................................................................ 6
  3.2.2 Certification Authority ............................................................................ 6
  3.2.3 SWIFTNet Directory .............................................................................. 6
  3.3 Keys ............................................................................................................. 6
  3.3.1 Key generation ........................................................................................ 6
  3.3.2 Key Storage ............................................................................................ 6
  3.3.3 Digital Signing and Encryption ............................................................... 7
  3.3.4 Non-repudiation of emission ................................................................. 7
  3.4 Digital Certificates ....................................................................................... 7
  3.4.1 Validating Certificates .......................................................................... 7

4 Certificate Administration ............................................................................... 8
  4.1.1 Registration ............................................................................................ 8
  4.1.2 Who Gets Certified ................................................................................. 8
  4.1.3 Preparing for Certification ................................................................. 8
  4.1.4 Certification ........................................................................................... 9
  4.1.5 Preparing for Recovery ....................................................................... 9
  4.1.6 Recovery ............................................................................................... 9
  4.1.7 Revocation ............................................................................................ 9
  4.1.8 Disabling .............................................................................................. 9
  4.1.9 Offline requests ................................................................................... 9

5 Operational Requirements ......................................................................... 10
5.1 Platform Support .......................................................................................... 10
5.2 COTS Products ............................................................................................ 10

6 Additional Services ..................................................................................... 10
6.1 Support Services ........................................................................................ 10

7 Glossary ....................................................................................................... 11
7.1 Acronyms and Abbreviations .................................................................... 11
7.2 Definitions ................................................................................................. 11
1 An Introduction to SWIFTNet PKI

SWIFTNet PKI is the mandatory SWIFT product required to secure the SWIFTNet services. It is installed alongside SWIFTNet Link. SWIFT’s portfolio of interactive communication services and related products include the interface products SWIFTAlliance Gateway and SWIFTAlliance WebStation.

It provides business applications with authentication, non-repudiation, integrity, confidentiality and access control capabilities.

SWIFTNet PKI and SWIFTNet Link are both mandatory components that, together, enable you to use the SWIFTNet services that SWIFT offers through its Secure IP Network.

SWIFTNet PKI provides a set of Application Programming Interfaces (APIs) that are directly usable by the application program. These APIs allow the customer application program to use the cryptographic and access control functions as well as obtaining and managing digital certificates.

SWIFTNet PKI also provides an end-user application for obtaining and managing digital certificates.

![Diagram of SWIFT portfolio of communication services]

*Figure 1 – SWIFT portfolio of communication services*
2 Value for Customer

2.1 General
SWIFT’s public key infrastructure (PKI) service issues digital certificates to financial institutions and corporates, thereby enabling a trusted, provable and confidential end-to-end communication over SWIFTNet.

Digital certificates provide the highest levels of authentication for institutions, end-users and servers. They convey trust both between institutions and with SWIFT (as the trusted third party).

2.2 Trust
The basic underlying principle of PKI is the chain of trust. It starts with the correspondent’s identity, based on the certificate’s validity, and ends with the digital signature.

The receiver of a signed message has trust in the originator’s identity of a message and the originator’s inability to repudiate the message because of the following guarantees:
- Strong process of subscribing the users to the SWIFTNet PKI
- Reliable process of issuing the certificates to the subscribers
- Virtual impossibility of producing a fake certificate
- Virtual impossibility of reproducing the signature from the certificate information
- Obligation to immediately revoke compromised certificates
- Validation of the certificate status at the message reception
- Link between the digital certificate and the message contents through the digital signature.

The level of trust in a certificate is set by the strength of the registration and revocation processes. SWIFT’s strong registration and revocation processes are based on the SWIFTNet PKI Service Description. This document translates the rules, roles and responsibilities into the actual PKI process with its specific procedures, rules and Service Level Agreements. It is an integral part of the contractual relationship between customers, and between customers and SWIFT. The certificates issued by SWIFT explicitly refer to the SWIFTNet PKI Service Description.

In the event that trust is compromised, SWIFT has a strong revocation process in place. Trust may for example be compromised under the following circumstances:
- when a smart card is stolen or a password is detected (private key exposure)
- when the relationship between the certificate owner and the Registration Authority is broken (employee leaving the company)

In such cases, the certificate containing the corresponding public key needs to be declared invalid and it must be revoked or disabled immediately.

2.3 Guarantees
The User can assume the following guarantees for the issued certificates:
- Authenticity
  Customers are guaranteed the identity of the originator of any instruction, statement, query or response. By verifying the signature, the receiver of a message can confirm that the sender specified in the header of the message owned the private key used for signing the message.
- Integrity
Customers are guaranteed that the data they receive exactly matches the original as produced by the sender. By verifying the signature, the receiver of a message can confirm that the message content has not been changed during transmission.

- **Non-repudiation of emission**
  Customers are able to prove that the claimed originator has effectively signed the message. This is because the originator is the sole owner of the unique signing key needed to produce the digital signature. This guarantee is dependent on the ability to revoke a certificate, whereby the time of the revocation request can provably be related to the time the message was signed.

- **Access Control**
  The access for an individual to his or her private key, which is stored in a smart card, is coupled to the access to SWIFTNet and is controlled through a private password.

- **Confidentiality**
  Optional message-level encryption guarantees that only the intended recipient can read and interpret the data. This is because the recipient is the sole owner of the unique decryption key.

The PKI-based digital signature replaces the message authentication code (MAC) used on today’s financial networks.

### 2.4 A Strong PKI

Before obtaining a trusted certificate, institutions are registered and certified by SWIFTNet PKI. This SWIFTNet PKI registration and certification guarantees a:

- **Clearly Defined Registration Process**
  Before they gain access to SWIFT’s Services, including SWIFTNet PKI, institutions are carefully screened. The screening is based on the admission criteria set down in SWIFT’s by-laws. In addition, Security Officers are only admitted under defined conditions, have limited capabilities and, where possible, work in pairs.

- **Responsive configuration environment**
  Fast set-up of end-users and fast revocation of compromised certificates are requirements for a high-level trust system. SWIFTNet PKI offers an online facility for managing end-users and their certificates and validating them.

- **Rigorous responsibility and liability (R&L) framework**
  To be able to accept liability for the PKI processes, both SWIFT and the user commit to a strong R&L framework. In order to accept liability for error, fraud and omissions, SWIFT implements rigorous internal procedures and software qualification criteria.

- **Complete security of key components**
  The Certification Authority is physically and operationally protected and isolated from other services. In addition, communication with the Certification Authority is only possible from certified Registration Authorities using a strong and secure protocol. The availability of the Certification Authority and the SWIFTNet Directory is critical to the certificate revocation service. It is guaranteed through a high degree of system redundancy.

- **Strong cryptographic environment**
  SWIFT uses algorithms with maximum practical key lengths. Moreover, where possible, private keys on the server, as well as on the client side, are generated and stored in hardware and are protected through passwords.
This strong PKI provides the 'best-of-breed' protection and trust for financial communication, which is particularly important in an interactive and transactional environment. It offers provable authenticity of messages, non-repudiation of the origin of messages, trusted time stamps and individual encryption of messages.
3 Features and Functions

3.1 PKI Client Components

The PKI client interacts with the central SWIFTNet PKI servers, that is, the Registration Authority (RA), the Certification Authority (CA) and the SWIFTNet Directory service operated by SWIFT. The PKI client consists of APIs for the cryptographic and certificate management functions and of a ready-made Local Registration Application for certificate management.

This is illustrated in Figure 2.

![Figure 2 – Client interaction with SWIFTNet PKI servers](image)

3.1.1 Local Registration Application

The Local Registration Application (LRA) is provided by SWIFT as an application or is provided by a third party based on the SWIFTNetLink APIs.

With the LRA the customer can:
- Register new users
- Revoke users’ certificates
- Disable users and remove their certificates from the SWIFTNet Directory

This application also controls the users’ access to the system and to their keys as well as providing password management.

3.1.2 Cryptographic and Certificate Management APIs

The cryptographic API provides the message security:
- Signing of messages, entirely and/or partially
- Signature verification and certificate validation
- Encryption of messages, entirely and/or partially
- Decryption of messages
- User certification
- Automatic key and certificate renewal
- User key and certificate recovery

The certificate management API provides the same functionality as the LRA.

### 3.2 PKI SWIFT Components

#### 3.2.1 Registration Authority

The Registration Authority (RA) has a central role in setting up the chain of trust. It is responsible for subscribing the institutions to the SWIFTNet PKI and delegating the subscription of additional users. The initial subscription includes the registration of the first two Security Officers (SO), who then use the Local Registration Application for their own certification and for issuing additional online certificate management requests to the RA.

#### 3.2.2 Certification Authority

The CA produces the certificates and publishes them in the Certificate Directory. This is done when requested by the PKI client and after validation by the RA.

The CA system is located in strongly protected buildings at the SWIFT Operating Centres. Equally, personnel access to the system is strongly protected. For redundancy reasons the CA consists of multiple systems located in different geographical regions.

#### 3.2.3 SWIFTNet Directory

The SWIFTNet Directory has an X.500 compliant hierarchical structure. It contains:
- Users’ signing and encryption certificates
- Users’ names and attributes
- Certificate revocation lists

The Local Registration Application can monitor the SWIFTNet Directory contents within the scope of its own institution. The cryptographic API of the PKI client can retrieve certificates from the Directory or can consult the Certificate Revocation List.

The CA and RA can only create or modify the SWIFTNet Directory contents.

### 3.3 Keys

#### 3.3.1 Key generation

PKI is based on asymmetric key pairs. In the SWIFTNet PKI, two separate key pairs are generated: one key pair for signing and another for encryption. Each pair consists of a public and private key.

The public keys are certified by the CA and are published as certificates in the Certificate Directory. The private keys are under the exclusive ownership of the user. The user must take care of their privacy.

The keys are created during the certification process and have a length of 1024 bits. The key renewal and expiry dates are defined in the Certification Practices Statement.

#### 3.3.2 Key Storage

In order to preserve the non-repudiation concept, the private signing key must not be exposed and therefore must never leave its storage medium.
The keys are stored in hardware. Smart cards for keys owned by a person and on disk for keys used by an application. In the near future, hardware security modules (HSM) will be available as a storage medium. The keys are protected with a password. The smart cards, card readers and the HSMs are standard products, available on the market and qualified by SWIFT.

3.3.3 Digital Signing and Encryption
In the SWIFTNet PKI the single holder of the private keys can sign and decrypt messages. Correspondents use the public keys, contained in the certificates, to verify the signature or to encrypt messages.

3.3.4 Non-repudiation of emission
Signed messages convey the proof of origin since the owner of the private signing key can only produce the signature.

3.4 Digital Certificates
A certificate is an electronic file signed by the CA that irrevocably identifies the owner of the keys and actually contains the public key. It guarantees that the owner is in possession of the corresponding private key. The SWIFTNet PKI provides each user with signature verification and an encryption certificate.

Amongst other things, a certificate contains the:
- Identity of the owner
- Identity of the issuing CA
- Certificate Serial Number
- Public key
- Start date and expiry date
- Policy ID for Business Certificates
- CA signature

The SWIFTNet PKI certificates comply with the X.509 format, are of version 3 and are stored in the SWIFTNet Directory.

3.4.1 Validating Certificates
The certificate must be efficiently retrievable. Therefore the relying user must be in direct communication with the directory. This directory must be authentic, meaning that user must be able to verify it is Swift's directory.

- The CA certificate must be authentic. Therefore the relying user must verify the CA signature on the CA certificate by using the CA certificate and by verifying the fingerprint.
- The CA certificate must be valid. Therefore the relying user must check the certificate start and the expiry dates. Also, the user must check that the certificate has not been revoked.

These functions are provided automatically by the PKI client.
4 Certificate Administration

The Security Officers use the LRA for certificate administration within the scope of their institution. Both the Security Officer and the user use the LRA for obtaining their certificates. This is illustrated in Figure 3:

![Figure 3 – Certificate Administration](image)

4.1.1 Registration

Security Officers create users in the SWIFTNet Directory. These users may then be certified. SOs identify the users by assigning them a formal X.500 name, the “Distinguished Name”. The user gets the status registered only after being defined in the SWIFTNet Directory.

4.1.2 Who Gets Certified

The institution decides who or what gets certified. Typically certificates are issued to employees or business entities, like departments. The certificates are then used by the individuals or by applications on behalf of the business entities.

4.1.3 Preparing for Certification

In this step, the Security Officer requests the RA to set-up a registered user for certification. The CA sets the status of the user to ready for certification, and it generates the activation secrets that the user will need in the certification process. The RA returns these activation secrets to the Security Officer, who passes them to the user.
4.1.4 **Certification**
To certify themselves, end users apply the activation secrets received from the Security Officer. The key pairs are generated and the public keys are certified by the CA. The user's signing and encryption certificates are published in the SWIFTNet Directory.

4.1.5 **Preparing for Recovery**
If users lose their keys or password, then the Security Officer will request the RA to set up the user for recovery. The CA will then generate and return new activation secrets that the user will need in the recovery process.

4.1.6 **Recovery**
Just like certification, the user initiates the recovery process if he or she has been prepared for recovery. The successful recovery results in new keys and the two new certificates are published in the SWIFTNet Directory.

4.1.7 **Revocation**
The Security Officer must revoke certificates whenever the trusted relationship with their owner is broken. This is mainly because the key has been compromised, for example, when passwords, smart cards or keys have been lost or stolen. Revoking certificates makes them unusable. Revoked certificates are published in the Certificate Revocation List in the SWIFTNet Directory. If desired, the user can be recovered after the revocation.

4.1.8 **Disabling**
By disabling a user, the Security Officer discontinues the automatic renewal of certificates and removes them from the SWIFTNet Directory. This is typically the case for users who no longer need their certificates.

4.1.9 **Offline requests**
In case the Security Officers are not able to perform an online user revocation or recovery, SWIFT needs to be contacted for a manual intervention. Any Security Officers registered at SWIFT can request SWIFT for a manual intervention.
5 **Operational Requirements**
The prerequisite components for obtaining SWIFTNet PKI possibly embedded in the SWIFTAlliance WebStation or SWIFTAlliance Gateway, are SWIFTNet Link and either SWIFTNet FileAct or SWIFTNet InterAct.

The operating requirements for SWIFTNet PKI are defined by, and are the same as, those required for SWIFTNet Link.

Please refer to the SWIFTNet Link Product Overview for more information.

5.1 **Platform Support**
The SWIFTNet PKI API and the Local Registration Application are available on the platforms on which SWIFTNet Link is supported. Please refer to the SWIFTNet Link Product Overview for more information.

5.2 **COTS Products**
The following COTS product forms part of the SWIFTNet PKI:

- Entrust Technologies
- Datakey Smart Card Reader, Model 10SR
- Datakey Smart Card, Model 330

6 **Additional Services**

6.1 **Support Services**
SWIFT Customer Services can provide first line helpdesk support, as well as service-specific second-line support. This service can be provided 24 hours a day, seven days a week, in a variety of local languages by highly skilled and experienced staff.

First line support centres are located in The Netherlands, U.S.A., Japan and Hong Kong. The product-specific second-line teams are based in New York, La Hulpe (Belgium) and Hong Kong. A world-wide problem management and tracking system ensures all customer calls are logged and tracked until the customer confirms closure.

In addition to these support services, SWIFT can also provide implementation and specialised consulting services, tuned to the individual needs of a customer.
7 Glossary

7.1 Acronyms and Abbreviations

API Application Programming Interface
CA Certification Authority
COTS Commercial off-the-shelf
CRL Certificate Revocation List
DN Distinguished Name
GUI Graphical User Interface
HSM Hardware Security Module
LRA Local Registration Application
PKI Public Key Infrastructure
RA Registration Authority
SNL SWIFTNet Link

7.2 Definitions

| Authentication                                      | A process used to ensure a person is who she/he claims to be or prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. |
| Certificate                                        | A unit of information contained in a file which, at a minimum, lists its issuer, a public key, indicates a user who holds the private key corresponding to the listed public key and is digitally signed by the certification authority. |
| Certification Authority                            | A central system at SWIFT for producing and publishing digital certificates. |
| Certificate Practices Statement                    | The statement of the practices that SWIFT Certification Authority employs in issuing certificates. |
| Certificate Revocation List                        | The list of all revoked certificates published by the SWIFT Certification Authority in a central directory and made available online to all PKI clients. |
| Encryption                                         | Making the contents of a message unreadable by enciphering it. Decryption has the reverse effect. |
| Local Registration Application                     | The application that the Security Officer uses for registering institution's users and for managing their certificates. |
| PKI Cryptographic module                           | The software at the customer side for securing messages and managing certificates. It performs the actual signing, signature verification, encryption and decryption and manages the unique private key of the customer and his certificates. It is delivered as part of the SWIFTNet Link product. |
SWIFTNet PKI

<table>
<thead>
<tr>
<th>Public Key Infrastructure</th>
<th>The infrastructure required to offer security services based on asymmetric cryptography.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Authority</td>
<td>A body at SWIFT that is responsible for the identification and authentication of the institution and the initial users of SWIFT’s PKI, such as the institutions’ Security Officers.</td>
</tr>
<tr>
<td>Security Officer</td>
<td>Person responsible for handling security matters for the financial institution.</td>
</tr>
<tr>
<td>Signature</td>
<td>A mathematical result calculated from a unit of digital information and a private key, such that one having the unit of information and the corresponding public key can, through verification, accurately determine (1) whether that mathematical result was created using that private key, (2) whether the unit of information has been altered since that mathematical result was calculated. The PKI-based digital signature replaces the message authentication code (MAC) used on today’s financial networks.</td>
</tr>
</tbody>
</table>

**SWIFTAlliance**

SWIFT’s brand name for the range of interface products to connect to the SWIFT services.

**SWIFTNet**

SWIFT’s brand name for all network and transaction processing services.

**SWIFTNet Directory**

The infrastructure allowing the SWIFTNet Link to lookup and retrieve various customer users and their public attributes. These include X.500-format distinguished names, Encryption and Verification Certificates (that is, Public Keys), revoked certificates and the CA Signing Certificate.

**SWIFTNet FileAct**

SWIFTNet FileAct is the file transfer service supporting the exchange of files containing bulk data.

**SWIFTNet InterAct**

SWIFTNet InterAct enables secure, real-time interactive communication between two parties across the Secure IP Network.

**SWIFTNet Link**

SWIFT’s mandatory software product to access all SWIFTNet services. SWIFTNet Link connects the customer to the SWIFTNet services.

**SWIFTNet PKI**

SWIFT’s mandatory security software and hardware installed alongside SWIFTNet Link.