Danske Bank Group

Certificate Policy

Document history

Version	**Date**	**Remarks**
1.0	19-05-2011	Version 1.0 finalized
1.01	15-11-2012	URL updated after web page restructuring.

Table of Contents

1. Introduction

This document is the Certificate policy (CP) of Danske Bank Group.

This document defines the rules by which keys and digital certificates are to be issued and managed by the Danske Bank Group Certificate Authority (CA) to its community of internal and external users with common security requirements.

Danske Bank Group is a northern European financial services provider, providing services in Denmark, Finland, Norway, Sweden, Ireland, United Kingdom and Luxembourg. Danske Bank Group CA is the root CA with country specific sub CA's in the hierarchy supporting services for subscribers in relation to their respective banks.

Danske Bank Group issue administration services, which address CA functions for subscribers. The services is in this document referred as CA administrative services.

Danske Bank Group deliver specific financial services for subscribers, using certificates issued under this CP, these services is in this document referred as financial services.

This Certification policy is structured to address financial services, taking EPC certification policy requirements augmented with certain sections of ETSI TS – ESI frame work with the following exceptions:

- Normally there should be references to a more detailed CPS document. Since this has yet to be developed, these are not included;
- There is no mention of certificate revocation procedures since given the nature of the financial services, this is not necessary;
- There is no mention of "relying parties" in the document since only CA and subscribers are involved in the transactions covered by the certificates; and,
- The CA is not subject to audits under ISO 27006.

2. Policy administration

2.1 Overview

This document describes the certificate policy (CP) which is applicable to all subscribers using financial services. This CP is subject to version changes from time to time. The CP and the archived versions can be found on **http://www.danskebank.com/en-uk/ci/Products-Services/Transaction-Services/business-systems2/Pages/PKI-Services.aspx**

2.2 Document name and identification

This CP is referred to as the "Danske Bank Group Certificate policy". All Certificates issued by the CA are issued pursuant to this CP.

2.3 Contacts

The contact person in relation to this policy is:

Poul Otto Schousboe
Ejby Industrivej 41
2600 Glostrup
Phone +45 45 14 19 52
Mobile +45 25 26 73 50
pos@danskebank.dk

2.4 Applicability

The certificates issued in accordance with the present CP may only be used by the subscribers for financial services. The certificates are provided for the purposes of non-repudiation, confidentiality, integrity and authentication.

Certificates cannot be used for anything other than financial services. Certificates must not be used for illegal purposes.

3. References

ETSI TS 102 042 v 1.2.1. (2005-05):"Electronic signatures and infrastructures; Policy requirements for certification authorities issuing public key certificates".

ETSI SR 002 176 V1.1.1 (2003-03): "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".
EPC291-09 V 1.0 (2009-11): "Requirements and Specifications for EPC Approved Server CAs for e-Mandate Services".

ISO/IEC 27002 (2005): "Information technology -- Security techniques -- Code of practice for information security management"

ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

FIPS PUB 140-2 (2001): Federal Information Processing Standard Publication -- "Security Requirements for Cryptographic Modules"

CWA 14167 -2 (2004): CEN Workshop Agreement -- "Security requirements for trustworthy systems managing certificates for electronic signatures"

4. Definitions and Abbreviations

4.1 Definitions

Certificate policy: A higher level statement with a set of rules that indicates how a certificate should be issued and used, and the obligations and liabilities of the entities involved.

Certification practice statement: A specification of procedures and controls that a CA applies when issuing certificates.

Certificate authority: An authority trusted by subscribers and relying parties, who has been authorized to generate, sign, issue and manage certificates.

Registration authority: An entity that is responsible for the identification and authentication of certificate subjects, but that does not sign or issues certificates.

Digital certificate: The public key of a subscriber, together with the identity and some other information, rendered unforgeable by encipherment with the private key of the CA issuing the Certificate.

Digital signature: Data in electronic form, which is attached to or logically associated with other electronic data and which serves as a method of authentication and integrity of that data.

Subscribers: An entity that signed a contract with CA to have them issue digital certificates with the intention of receiving services and/or products.

Confidentiality: The information security principle ensuring that remaining information is accessible only to those authorized to have access.

Non Repudiation: The principle that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Integrity: In information security, integrity means that data remains intact through the whole process without being altered.

Authentication: The process of establishing identity based on the possession of a trusted credential.

4.2 Abbreviations

CP	Certificate Policy
EPC	European Payments Council
ETSI	European Telecommunications Standards Institute
ESI	Electronic Signatures and Infrastructures
TS	Technical Specification
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment
CA	Certificate Authority
HSM	Hardware Security Module
EDI	Electronic data interchange
CPS	Certificate practice statement
CRL	Certificate revocation list

4.3 Notations

The requirements contained in this CP include:

Compulsory requirements, which must be met. Such requirements are stipulated using the term "must".

Requirements, which should be met. Non-fulfillment of such requirements must be reasoned. Such requirements are stipulated using the term "should".

5. Concepts

5.1 Certificate authority (CA):

The Danske Bank Group certificate authority is an entity that issues digital certificates and acts as a trusted third party for users and parties relying on the certification services. The CA has the overall responsibility for the provision of services that are necessary to issue and maintain certificates.

5.2 Registration authority (RA):

The Registration authority (RA) is an entity responsible for the identification and authentication of certificate subjects, but that does not sign or issue certificates.

In the Danske Bank Group Public Key Infrastructure (PKI), Danske Bank Group RA's are operating under the control and authority of CA and accept Danske Bank Group certificate applications from subscribers.

Danske Bank Group RAs must authenticate the identity of the Danske Bank Group certificate subjects and must perform verification of the information contained in the application. If the verified information is correct, the RA sends a certificate request to CA to issue a Danske Bank Group certificate for the subject.

5.3 Certification services:

The following services are provided according to this certification policy:

R*egistration:* The registration authority (RA) verifies the identity of the subject and any specific attributes.

Certificate generation: The subscriber's generate key pairs on their computer using software or a HSM. The public key generated by the subscriber is signed by the CA

Dissemination service: The subscriber's public key signed by CA is disseminated to the subscribers through certificate generation service.

Certificate revocation: Reception and handling of requests for cancellation of certificates.

Certificate status*:* The status of certificates connected with financial services is verified through CA administrative services.

5.4 Subscriber and subject:

Subscribers are parties who enter into a Customer Agreement with Danske Bank Group for the issuance of Certificates from the CA.

Subjects are entities such as individuals, organizations or devices and systems, which act on behalf of a subscriber.

5.5 Relying parties:

Due to the bilateral nature of this service subscribers connected through financial services rely on certificates issued by the CA. There are no other relying parties involved.

6. Responsibilities, liability and conformance

6.1 Responsibilities

6.1.1 Certification Authority obligations:

In relation to activities conducted under this CP the CA must:

- Ensure that all requirements detailed in section 7. of this document are implemented;
- Ensure that the affiliated RA complies with its own obligations;
- Ensure issued certificates are available for all parties using financial services;
- Accept and confirm revocation requests from entities requesting a certificate to be revoked and make the CA root certificate status available;
- Ensure that a private key is used for issuing certificates to the subjects and issuing certificate revocation status information; and,
- Comply with audit requirements set out in section 6.3, to ensure that the procedures used comply with this CP;

6.1.2 Subscribers' obligations:

Subscribers must have an agreement with the CA, which sets out the following obligations:

- Provide information to the CA that is accurate and complete, to the best of the subscriber's knowledge and belief, regarding information in their certificates and identification and authentication information and promptly notify the CA of any changes to this information or errors in certificates issued.
- Generate, store and use the signing and encryption certificates as directed by the CA.
- Promptly notify if the subscriber has reason to believe that the secret key is compromised, lost or the subscriber no longer needs the certificate.
- Protect the certificate and private key with a password and ensure possible back-up copies of the private key are maintained in a secure manner.
- Inform CA promptly, if private keys are generated and kept outside HSM crypto hardware.

- Use the certificates exclusively for the agreed purpose in accordance with the CP.

6.2 Liability

Issuing and maintaining this CP is part of Danske Bank Groups efforts to standardize and formalize existing cooperation and usage of security in the products grouped under the name “financial services”.

Liability as such as therefore given in and follows the agreements set up between Danske Bank Group and each customer concerning the use of each particular financial service.

6.3 Conformance

The CA must claim conformance to the present certificate policy which is identified in the certificate that it issues if it has a current assessment of conformance to the identified certificate policy in the issued certificates. The assessment can be an audit report from internal auditor who is independent of the CA functions and the assessment report should be made available to the subscribers.

If the CA is non-conformant at any stage; it should stop issuing certificate with this policy identifier and resolve the non-conformance within a reasonable period of time.

The CA’s compliance must be checked on a regular basis and whenever a major change is made to the CA.

The conformant CA must demonstrate that it meets its obligations detailed in this policy and implemented controls which meet the requirements. The areas where these controls need to be detailed are specified in section 7 of this document.

7. Certificate authority practice requirements

7.1 Public key infrastructure – Key management life cycle

7.1.1 CA key generation

The CA key must be generated in controlled circumstances as per the following requirements.

- The CA root key and encryption key should be generated in a secure environment by a minimum of two trusted personnel who are authorized to perform CA functions.

- The CA key generation must be carried out in a cryptographic module which meets one of the following requirements:

  - FIPS PUB 140-2, level 3 or higher,
  - CEN Workshop Agreement – CWA 14167-2 or higher,
  - A trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408

- The CA root key must be generated using the industry recognized algorithm (RSA) with a minimum key length of 2048 bit. The CA encryption key must be generated with a minimum of 1024 bits.

7.1.2 CA key storage, backup and recovery

The CA must ensure that CA root key and encryption key are stored and backed according to the following requirements.

- The CA root key and a backup copy must be stored and used in secure cryptographic modules which meets one of the following requirements:

  - FIPS PUB 140-2, level 3 or higher,
  - CEN Workshop Agreement – CWA 14167-2 or higher,
  - A trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408

- The CA’s root key and encryption key must be stored, backed up and recovered in a secure environment by a minimum of two trusted personnel who are authorized to perform CA functions.

- The CA’s expired or revoked signing key must be destroyed or archived.

7.1.3 CA public key distribution

The CA’s public key is delivered to subscribers in a signed zip file (using a dedicated VeriSign certificate), which can also be downloaded from bank homepage. As an alternative method this zip file can also be emailed directly to subscribers.

7.1.4 CA key usage

The CA must maintain controls to provide reasonable assurance that CA keys are used only for the intended functions of:

- Signing certificates
- Updating the Certificate Status

7.2 Public key infrastructure - Certificate management life cycle

7.2.1 Subject registration

The CA must ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are examined and verified through authorized sources.

The CA requires that the subscriber submit the certificate request form and the RA must verify the identity of the subscriber as per the following process:

- A personal subscriber states his/her name and civil registration number. Organizational subscribers state the name of the organization and the number according to the national organization register.
- The RA verifies the subscriber’s identification through national register or the national organization register.
- If the subscriber is already an existing customer, the verification process may deviate from the above process.

Before entering into a contractual relationship with a subscriber, the CA must inform the subscriber of the terms and conditions regarding use of the certificate as given in section 7.2.4

If the subject acting behalf of a subscriber is an individual, the subject must be informed of his/her obligations.

The subscriber must provide a physical address and contact details, which describe how the subscriber may be contacted.

The CA must record the signed agreement with subscribers which should include:

- The CA’s right to retain information used in registration,
- The subscriber’s agreement on its obligations,
- The CA’s right to process the subscriber’s identity information whilst it is being verified.

The CA must retain the subscriber’s application records for the period of time required by law for the purpose of providing evidence of certification in legal proceedings.

7.2.2 Certificate renewal, rekey and update

The CA maintain controls to provide reasonable assurance that only accurate and authorized certificate renewals are processed by:

- Status verification function to verify the expiry date of the certificates
- Provide renew function to generate new certificates. Requests to renew a certificate are only processed if the subscriber already has a valid certificate.

When a subscriber certificate has been revoked or has expired, the subscriber will need to undergo the registration process to obtain a new certificate.

7.2.3 Certificate Generation

The CA’s certificates are generated on dedicated IT systems within a Hardware Security Module (HSM).

On the basis of certificates issued by the CA, subscribers generate two certificates, one for signing and the other for encryption. Subscribers generate these certificates on their own systems according to requirements set out by ETSI SR002 176 and FIPS 140-2 level 2 compliance.

The CA recommends that subscribers generate and store the keys using a HSM instead of software.

The subscribers must generate a key pair using an algorithm and key length approved by the CA. Any request for key length less than the approved length will be rejected.

In the certificate generation process the following attributes should be included in the certificate:

- Identification of the issuing CA and the country in which the CA is established;

- Information relating to the holder of the certificate;
- The identifier of the holder;
- Certificate issue and expiry dates;
- Certificate unique identification number (serial number);
- Reference to this CP (OID);
- The public key of the holder; and
- The CA's electronic signature.

7.2.4 Dissemination of terms and conditions

The CA must ensure that the terms and conditions are made available to subscribers regarding the use of the certificate, by communicating the following:

- The CP being applied*;*
- Any limitations on the certificate use;
- Subscribers obligations;
- The CA's liability limitations ;
- Terms for retaining the subscriber's registration information , and,
- The applicable law.

The terms and conditions must be available through a durable means of communication, which may be transmitted electronically or physically and must be understandable by all the entities involved.

The CA must inform the subscriber that the private key must not be used for signing following a request for revocation or a notification of revocation, or following expiry.

The CA must inform the subscriber that the issued certificate cannot be used to sign other certificates.

7.2.5 Certificate revocation and suspension

The CA does not support suspension services.

The CA must revoke a subscriber certificate under the following circumstances:

- The subscriber requests revocation, because they no longer need the service;
- The subscriber forgot the private key password;
- If there is a change in subject's attributes;

- The subscriber requests revocation because the private key is compromised or suspected to have been compromised;
- Death of the subject.
- If the subscriber violates their obligations or the terms and conditions defined under this CP.

The subscriber requesting the revocation must be authenticated. The authenticated request could be a message digitally signed by the subscriber with a valid signing key. In case of any alternative method the subscriber should prove their identity.

The CA must revoke the subscriber's certificate within 24 hours following receipt of a revocation request.

7.3 CA management and operation

7.3.1 Security management

CA maintains information security and implements controls as per the industry recognized standards, ISO/IEC 27002.

The CA management must maintain a security policy to provide directions on information security.

If the CA outsources the management and control of all or some of its information systems to a subcontractor, the security requirements of the CA are addressed in the related contract and the CA has ultimate responsibility for compliance.

The CA must carry out a risk assessment to evaluate business risks and determine the necessary requirements and operational procedures.

Security controls and operating procedures for CA facilities, systems and information assets providing the certification services must be up to date and documented. Any changes to the CA system should be authorized and go through a change management process.

7.3.2 Operations management

The CA maintains controls to provide reasonable assurance that secure operations of CA information processing facilities are secured and the risk of system failure is minimized.

Damage to the CA's information processing facilities from security incidents and malfunctions must be minimized through the use of incident management process.

The CA must implement procedures to evaluate capacity management for information systems involved with CA operations.

The CA maintains controls to provide reasonable assurance that media are securely handled to protect media from damage, theft, and unauthorized access.

The CA must implement procedures for all trusted and administrative roles that impact the provision of certification services.

7.3.3 System access management

The CA must limit access to CA systems to appropriately authorized individuals.

The CA’s internal network should be separated and protected by configuring and maintaining firewalls.

The CA must have a process for user access administration in relation to applications, databases and operating systems connected with the CA services. Controls should be implemented to ensure that individuals only have access to required resources.

The CA’s systems should be enabled with event logging to enable traceability and accountability.

7.3.4 Business continuity management

The CA must maintain a business continuity plan to provide reasonable assurance of continued operations.

Business continuity plans must be tested regularly to ensure that they are up-to-date and effective.

In the event of incident/disasters, the CA systems must be backed up in a secure place and should be restored to allow timely recovery of operations.

7.3.5 Compliance with legal requirements

The CA maintains controls to provide reasonable assurance that the CA complies with relevant legal requirements.

The CA must ensure that private information of subscribers is only used for the purpose required for operating the CA.

The subscriber’s information must not be disclosed without the subscriber’s agreement or other legal authorization.