Danske Bank CA

Certification Practice Statement – financial services, Finland

Document History

Version	Date	Responsible	Remarks
0.1	12-03-2012	JRGU	Draft based on former drafts.
0.1	09-10-2012	LGG	Comment and review
0.1	01-11-2012	AKT	Comments on Legal issues
0.2	12-11-2012	JRGU	Release candidate
0.3	03-12-2012	JRGU	Names and formalities adjusted.
1.0	03-12-2012	MIJAC	Published version 1.0
1.1	06-02-2015	MIJAC	Spelling corrected

Table of Contents

1 Introduction

This documents is the Certification Practice Statement (CPS) of the Certificate Authority DBGCAFI which issues certificates to Danske Bank customers in Finland utilizing the PKI web services provided by Danske Bank.
The Certificate Authority DBGCAFI is issued by the Danske Bank root certificate: DBGRoot.

Danske Bank CA is the authority that is associated with the issuance and management of digital certificates. Danske Bank CA operates the root CA DBGRoot, which is used to issue and maintain the country specific sub CA's in the hierarchy.

Danske Bank is a northern European financial services provider, operating in Denmark, Finland, Norway, Sweden, Ireland, United Kingdom and Luxembourg.

PKI web service is the administrative service of Danske Bank, which address CA functions to deliver Secure communication services for customers, based on PKI.

This CPS takes into account "Internet Engineering Task force (IETF) RFC 3647" and "ETSI TS 102 042 v 2.2.1" as sources of guidance with regards to standard practices in the area of electronic signature and certificate management.

Danske Bank issues CPs to describe sets forth requirements that Danske Bank financial services participants must meet ("what is to adhered to")
This CPS describes how Danske Bank CA fulfills these requirements (" How is it adhered").

Danske Bank CA operates at the same security level regardless of the certificates issued. This CPS describes this security level.

2 CPS Administration

2.1 Overview

This document describes the certification practice statement of Danske Bank Group CA Financial services Finland, (Certificate Authority DBGCAFI) which is applicable to all parties using financial web services from Danske Bank PKI Services.
This CPS addresses the technical, operational and management controls and procedures in all services during the complete life cycle of certificates as issued by Certificate Authority DBGCAFI, in accordance with the requirements of the Certificate Policies issued by Danske Bank Group
This includes that the certificates issued, shall only be used to access the Danske Bank PKI Services.

2.2 Document name and identification

This CPS is referred to as the "Danske Bank Group Certification Practice Statement – financial services, Finland".

OID : 1.3.6.1.4.1.3984.292082005.1.1.02

(http://www.danskebank.com/en-uk/ci/Products-Services/Transaction-Services/business-systems2/Documents/DB_CertificationPracticeStatement V1-1.pdf)

2.3 Changes & approval

The Danske Bank Group IT Security is responsible for reviewing and approving changes to CPS'es in the Danske Bank group.

2.4 Publication and distribution

This CPS is subject to version control from time to time, whenever there is a major change in operating procedures or functionality of the Danske Bank CA. The current version and archived versions will be communicated to the authorized parties operating PKI webservices site available to those needs to verify the certificates issued. The CPS is valid from date of publication until a new version is published.

Links to the CPS's provided by Danske Bank can be found at this site:

https://www.danskebank.com/en-uk/ci/Products-Services/Transaction-Services/business-systems2/Pages/PKI-Services.aspx

2.5 Contacts

The contact person in relation to this CPS is:

Head of Group Security Danske Bank.
Poul Otto Schousboe
Ejby Industrivej 41
2600 Glostrup
Phone +45 45 14 19 52
Mobile +45 25 26 73 50
Security@danskebank.dk

3 Identification & Authentication

3.1 Initial identity validation

Danske Bank CA Certificate Authority DBGCAFI only issues certificates to customers of Danske Bank Finland.
The identification of the customers are done according to the various legislation subject to the Anti Money Laundering directives and local regulation of requirements for identification of customers identity as applicable in Denmark and Finland.

3.1.1 Authentication of organization identity

Certificates are issued either at organizational level[1] or at employee level. First certificate is issued to the known contact person according to signed agreement.

3.1.2 Authentication of Individual identity

The authentication of the identity of the employees in an organization, is the responsibility of the organization itself. Danske Bank Finland base authentication of the certificates issued on the information claimed by the contact person in the signed agreement.

3.2 Identification and authentication for renew

Renewal is an integrated part of daily operations. Following the practices in the PKI web service description the certificates will be automatically renewed, when close to expiration.

3.3 Identification and authentication for renew and revocation request

Revocation is an integrated part of daily operations. The holder of a valid certificate has the administrative rights to revoke and renew certificates, issued to the certificate identity, by use of PKI web services.

4 Operating Procedures

[1] Certificates at organizational level identifies the organisation without identifying an individual. This might be used for automated communication with the PKI web services.

4.1 Certificate application and processing

Request for certificates in Danske Bank Finland, is done by filling out an Business Online and/or Web Services Communication Protocol and PKI Security Solution Agreement. Only customers in Danske Bank Finland can apply for the relevant certificate(s).
When the Business Online agreement has been accepted the customer receives an activation PIN code, by mail in a confidential envelope.

4.2 Certificate generation

The Customer ID and PIN code are used by the customer to access Danske Bank Group PKI web services to create a Certificate Authority DBGCAFI signed certificates.

The following steps are performed by the customer to create Certificate Authority DBGCAFI signed certificates.

1. Download Danske Bank root certificate (DGBRoot) archieve from URL.
2. Validate 3. Party signature signing the archieve.
3. Enroll root certificated in local keystore.
4. Generate two key pairs using software or hardware security module, HSM with minimum key length of 1024 bits.
   This is done according to recommendations in ETSI SR 002 176 V1.1.1 (2003-03). Danske Bank CA recommend use of a HSM module, the customer can choose to use software.

   Use the services GetBankCertificate and CreateCertificate described in [PKI service description[2]] for management and issuing of certificates.

In the complete certificate generation procedure, the private keys of the customer are never revealed to the bank or to anybody else. Only the customer has access to the private keys, and is able to sign the documents, and only the customer is able to decrypt messages encrypted with the customer encryption certificate.

4.3 Certificate renewal

To request the renewal of a Certificate Authority DBGCAFI certificate, customers may use the certificate management program RenewCertificate option through PKI web services.

Only customers with valid signing certificate are able to use RenewCertificate option.

By using RenewCertificate option, two certificates are issued - one for signing and the other for encryption, with a new serial number and validity date.

[2] PKI service description can be found at:
https://www.danskebank.com/en-uk/ProdServ/corporate/business-systems2/Pages/PKI-Services.aspx

4.4 Certificate revocation

Customers may request for revocation if they no longer need the service or if they suspect the private key of the certificate may have been compromised. The Danske Bank CA can revoke the issued certificates if the customers violate the terms and conditions of the subscription.

Customers can use RevokeCertificate option in certificate management program if their signing certificates are still valid. Once the RevokeCertificate option is executed, both the signing certificate and encryption certificate will be revoked.

Once a certificate is revoked, the customer needs to undergo a new registration process to obtain a new certificate.

Customers can also revoke their certificates by contacting the bank customer service and request revocation. In such cases the customer must present proof of identity for such revocation requests to be accepted.

4.5 Certificate status

Customers may verify the status of their certificates using CertificateStatusRequest, in the Certificate management program accessible through PKI web services.

Danske Bank CA Certificate revocation/status can be verified through the Certification Revocation List. Only bank certificates will be in the list. This CRL is updated every 24 hours, and is valid for 48 hours.

4.6 End of subscription and CA termination

Customers can end subscription at any time by revoking all the customers certificates or by terminating the signed Business Online and/or Web Services Communication Protocol and PKI Security Solution Agreement. In case of termination of a Certificate Authority DBGCAFI the CRL will state the CA certificate as revoked as well as all issued certificates issued by this CA.

5 Facility, management and operational controls

5.1 Physical security controls

The Danske Bank Group CA is integrated in the security infrastructure of the Danske Bank group.
As such the physical security is governed by the same measures as the financial systems maintained in this environment.

5.1.1 CA service center location and Physical access

CA services provided from Danske Bank Group CA is operated from Danske Bank locations in Glostrup, Denmark and the backup facility in Brøndby, Denmark.

CA is physical operated by an external contractor.

Physical access is restricted to trusted operators. Physical access will not give the operators access to issue certificates. Duplicated sites ensures continuation of the CA services, even in case of physical destruction of one site.

5.1.2 Power, cooling and fire

The physical security is redundant established with power backup, cooling and fire protection.

5.2 Procedural controls

Service operation processes of the Danske Bank CA is defined and documented by the internal department "34BE- Application Security Integration".
The operation of the Danske Bank CA is outsourced to the external supplier IBM.

5.2.1 Trusted roles in CA

Access to the facilities of the cryptographic environment including the crypto functionality and the crypto keys are segregated, by the requirement of dual persons must be present at the same time. Dual persons are required to logon to and to operate the crypto system.

5.2.2 Functional separation

The internal role based IAM system ensures that registration and authentication of customers are separated from service operator IBM, where the CA are operated.

5.2.3 Dual control

Functional separation ensures segregation of duties. One person cannot both authenticate the customer and issue certificates to the same customer. Physical and logical access requires the presence of two persons each holding part of the access key.

5.3 Personnel security controls

5.3.1 Qualification & Background verification

All employees have signed confidentiality agreement.
Internal training and instructions ensures employees qualifications.

5.4 Business continuity and Disaster recovery

Instruction are kept physical secure and ensures that service operation do not rely on single persons.

6 Technical Security Controls

This chapter describes the overall rules for generating keys and accompanying security controls for issuing Danske Bank CA root key, and underlying Danske Bank keys issued below the root key used in PKI services

6.1 Key pair generation and installation

All customer keys are generated in the customers equipment. The keys must be generated according to recommendations in ETSI SR 002 176 V1.1.1 (2003-03)The customer keys lifecycle is the responsibility of the customer. Danske Bank recommend customers to use certified crypto hardware for key store.

The CA keys in Danske Bank CA are generated in crypto HW, certified according to FIPS 140-1 level 4.

6.2 CA key protection and Backup

The CA keys in Danske Bank CA are generated in crypto HW, certified according to FIPS 140-1 level 4. The keys are cloned utilizing the facilities in the utilized equipment, and exists in dual locations.

6.3 Algorithms and Key length

CA keys are generated with at minimum key length 2048 bits.
Customer keys have at minimum key length 1024 bits, and are signed using sha256RSA.

6.4 Activation Data

Request for issuing a certificate based upon the customer keys, require usage of Customer ID and PIN code issued to the specific customer.
The customer certificate is active when the request is processed in the bank, within a few seconds from receiving the request.

7 Certificate and CRL Profiles

The certificates issued by Danske Bank CA to subordinate CA's and end entity certificates are in accordance with ITU-T standard - X.509 version 3.

7.1 Certificate profile

7.1.1 CA Certificate profile:

General attributes:

Attribute	Value

Internal label	DBGttcc
	Where tt = type of key used for PKCS#10 request:
	CA = dynamic keys (memory only)
	SW = software keys (file on disc)
	HW = hardware keys

	And cc = country DK – Denmark FI – Finland SE – Sweden NO – Norway LU – Luxembourg GB – United Kingdom IE – Ireland
Key length	2048 bit
Lifetime	10 years
Subject	DBGttcc
Key usage HSM	CA=true, Key Management=false, Signing=false, SSL=false
Issuer	Subject of DBGROOT
Key usage:	Certificate Signing, Off-line CRL Signing, CRL Signing
Organizational Unit (OU)	Contains "Danske Bank" followed by the name of the country used in internal label. DK – Denmark FI – Finland SE – Sweden NO – Norway LU – Luxembourg GB – United Kingdom IE – Ireland

7.1.2 Customer Certificate profile:

Two certificates are issued to the customer, one for signing and one for encryption.

General attributes:

Attribute	Value
Version	V3

Key length	CA = 1024 bit
	SW = 1024 bit default, 2048 bit possible
	HW = 1024 bit default, 2048 bit possible

Lifetime	Depends on key type:
	CA = 1 day
	SW = 2 years
	HW = 2 years

Issuer	Subject of CA Certificate
Subject Key Identifier	The Subject Key Identifier is calculated as a 'sha1' hash of the certificates public key.
Authority Key Identifier	Subject Key Identifier of CA Certificate
Signature algorithm	sha256RSA
Thumbprint algorithm	sha1

Signing certificate attributes:

Attribute	Value
Cert Serial	<14 digit sequential number>01
Key usage	Digital Signature, Non-Repudiation

Encryption certificate attributes:

Attribute	Value
Cert Serial	<14 digit sequential number>02 Note: sequential number is the same as used in the signing certificate.

Key usage	Key Encipherment, Data Encipherment

7.2 CRL profile

The Danske Bank Group CA will issue X.509 version 3 CRLs. This CRL is only updated with the CA certificate status/revocation information.

8 Definitions & abbreviation

Definitions and abbreviations used in this document is the common used terms regarding public key infrastructure.

9 References

Danske bank PKI service descriptions can be found at:
https://www.danskebank.com/en-uk/ProdServ/corporate/business-systems2/Pages/PKI-Services.aspx

Other referred documents are public available on the Internet.