Certificate Practice Statement

For the

Rabobank

Certificate Authority

Prepared By: CM

Rabobank

Contents

1 Introduction

Rabobank operates a Certificate Authority (CA), which issues public key certificates to internal and external Rabobank business customers for use in securing Rabobank business applications for use within the Rabobank internal namespace. The Rabobank CA does not supply certificates for use in the public namespace, Internet.

For certificates to be used on the Internet representing Rabobank, the Rabobank maintains contracts with two public CAs. Both internal and external CAs are operated by the same department, as a single point-of-contact for certificates.

This document will describe for users and stakeholders in Rabobank business applications the practices and procedures that the Rabobank Certificate Authority (Rabobank CA) utilizes in the conduct of CA service and operations. These practices consist of business and operational practices associated with the issuance and management of certificates.

The services and operations of the Rabobank CA are intended solely for Rabobank users and applications. The Rabobank CA is not intended to provide general certificate services for the general public, nor for any applications other than Rabobank applications.

1.1 Scope

This Certificate Practice Statement (CPS) document pertains solely to the business and operational practices of the Certificate Authority operated for the purpose of authentication of Rabobank business customers. This CPS does not pertain to any other Rabobank certificate authority system that may be in operation or contemplated in the future.

1.2 Purpose

The purpose of this CPS document is to objectively define the practices and procedures that the Rabobank CA utilizes in the conduct of CA service and operations. This CPS also defines the obligations and responsibilities that involved entities have in the conduct of creating and using certificates issued by the Rabobank CA. The intent of the CPS is to allow involved entities, such as the Rabobank business customers, to understand and review the practices of the Rabobank CA.

1.3 General Trust Model

The services of the Rabobank CA will support secure Web access to certain Rabobank business applications. To accomplish this, the Rabobank CA provides a trusted service for issuing and revoking, when duly notified, certificates in accordance with these published practices. The Rabobank CA provides a service that Rabobank business customers may rely on for the provisioning of certificate management services.

1.4 General Discussion of Certificate Issuing and Management

The Rabobank CA provides a service to facilitate the confirmation of the relationship between Rabobank business customers, Rabobank business management, and the Rabobank CA. The management process for certificates involves the acceptance of certificate requests, the appropriate authentication of requester identity, issuance of certificates, publishing of certificates into a repository (Directory), revocation of certificates and audit trail creation and maintenance.

1.5 Definitions

- Rabobank CA - Rabobank Certificate Authority.
- Applicant - A potential user of a Rabobank application that requires a Rabobank certificate. A Rabobank business customer will submit certificate requests on behalf of an applicant.
- Subscriber - A user of a Rabobank application that has been issued a Rabobank certificate

1.6 Certificate Types

The Rabobank CA supplies the following certificates:

1.6.1 Rabobank user certificate

This type of certificate is stored on smartcards as issued to internal users to authenticate to the network. The certificate is linked to the user via the email address. Physical smartcards are gradually augmented by virtual smartcards.

1.6.2 Rabobank device certificate

This type of certificate is intended to prove the identity of a device to the network and/or a cloud platform. This certificate is stored on the device and protected by local facilities.

1.6.3 Rabobank Web Server certificate

This type of certificate is intended for Rabobank servers to facilitate the establishment of Secure Sockets Layer connections between Rabobank operated Web servers, other devices, and client browsers.

1.6.4 Rabobank Code Signing certificate

This type of certificate is intended for Rabobank's use to apply a digital signature to Rabobank written applications.

1.6.5 Rabobank Intermediate Certificate

This type of certificate is intended for Rabobank's use to sign certificates through a trusted intermediate CA.

2 Obligations and Responsibilities

The Rabobank CA, Rabobank business management, and the Rabobank subscribers (users) have obligations and responsibilities with respect to the various facets of handling and using public key certificates and the supporting systems associated with certificate usage. These obligations and responsibilities are described below.

2.1 CA Obligations and Responsibilities

The Rabobank CA will have the following obligations and responsibilities:

Provide appropriate security for the certificate management process (including certificate issuance, certificate revocation and audit trails) and the protection of the CA signature key.

The Rabobank CA will ensure that there is no collision of the subscriber's name (as defined in the Distinguished Name on the subscriber's certificate) with that of any other Rabobank CA subscriber.

Certificates will be issued and available within a reasonable time after a properly formatted and validated Certificate Request is received by the Rabobank CA. There are subscriber obligations that affect the time required to validate the Certificate Request.

The Rabobank CA will maintain a process to ensure timely notification by e-mail of pending certificate expiration when renewal requires subscriber action.

The Rabobank CA will maintain a process enabling subscribers to request revocation of certificates in case of possible compromise.

The Rabobank CA will publish certificate validity information via the Certificate Revocation List (CRL) via the CRL Distribution Point (CDP). Rabobank business applications will check the CDP before accepting a certificate as valid.

2.2 Rabobank Business Management Obligations and Responsibilities

The management of a Rabobank business application, that requires a certificate, will have the following obligations and responsibilities:

Deliver correct information in the Certificate Request process in RCMP, the Rabobank Certificate Management Portal. RCMP validates this information with the CMDB.

When required, deliver appropriate information for the vetting process, when requested.

The Rabobank portal will initially process incoming Rabobank customer applications for certificates. After identifying the applicant as an authorized user of a Rabobank business application, forward the application to the Rabobank CA.

The Rabobank security contacts will notify the Rabobank CA when a subscriber's certificate is to be revoked.

2.3 Subscriber Obligations and Responsibilities

Subscribers to the Rabobank CA will have the following obligations and responsibilities:

The subscriber shall not divulge the value of any private key associated with that subscriber's certificate issued by Rabobank CA to any other entity.

The subscriber shall notify the applicable security contacts once any of the following conditions occurs:

- The subscriber no longer requires access to any Rabobank web-based business application or access to Rabobank facilities.
- The subscriber suspects his private key has been compromised.
- The subscriber forgets or no longer knows the password for their web browser.

The subscriber shall follow the official procedures and instructions distributed by the Rabobank business management related to requesting and retrieving of certificates.

The subscriber shall use certificates issued by the Rabobank CA solely for official business communications with the Rabobank.

3 Certificate Processing Procedures

This section of the CPS describes the procedures used by the Rabobank CA to authenticate and validate the identity of the subject named in a certificate request or revocation request received by the Rabobank CA.

3.1 Generating the Certificate Request

The applicant will submit a certificate application via RCMP to the Certificate Management contact responsible for Certificate Provisioning.

3.2 Certificate Request Authentication

Once a certificate request submitted by the applicant has been received in RCMP for processing, the CM contact will verify that the applicant's name is on the list of authorized business customers. The CM security contact will then verify the request for origin, validity and applicability. If any of the parameters is in doubt, CDC will contact the requester.

3.3 Processing Applications

The CDC security contact will forward all authorized applications to the Rabobank CA for processing. The Rabobank CA will prepare a wrapped certificate. The Rabobank CA will give the wrapped certificate to the Rabobank security contact. The Rabobank security contact will mail the following to the applicant: the wrapped certificate, a processed application with a reference number for certificate renewal, and instructions on how to retrieve and protect the certificate. The password to unwrap the certificate will be communicated via a third channel (SMS).

3.4 Certificate Revocation

Certificates will be revoked if any of the following events occurs:

3.4.1 The private key value or the password protecting the subscriber's private key is compromised (known to any other entity other than the subscriber)

3.4.2 The subscriber's employment or affiliation with the customer is terminated.

3.4.3 The subscriber no longer requires access to any Rabobank application

The Rabobank CA shall take immediate action to revoke a certificate for which the Rabobank CA is notified that the associated private key has been or might have been compromised. Once the Rabobank CA is notified of a known or suspected private key compromise, a certificate will be revoked within 2 hours.

4 CA Operational Practices

4.1 Official Rabobank CA Contact Point

Contact information (names of personnel, including several layers of backup, along with telephone numbers and e-mail addresses) will be supplied to subscribers by the Rabobank security contact in written documentation, which will be updated as required.

4.2 Audit Logs

The Rabobank CA maintains audit logs, which are updated in real time. These audit logs are protected from tampering. These logs are also backed up to physical media (digital tape). Copies of these audit log backup tapes are stored both onsite and off-site to facilitate recovery if necessary. Audit logs contain the full history of the operational activities of the Rabobank CA.

4.3 Disaster Recovery and Business Continuity

The Rabobank CA provides a backup capability to restore Rabobank CA functioning in the event of a system failure at Rabobank CA. It is anticipated that in the event of a full system failure, the Rabobank CA can be restored to service within 16 hours elapsed time.

4.4 Physical Security

The Rabobank CA server computer is protected by a variety of physical security controls which include card key access to the physical computer data center at multiple, layered entry points

4.5 Technical Security Controls and Key Management

4.5.1 Key Length

Rabobank root CA uses a private key/public key pair that is 4096 bits long.
The subscribers are required to use private key/public key pairs that are at least 2048 bits long.

4.5.2 Validity Period for Certificates (Key Life)
The validity period for certificates issued by the Rabobank CA has a maximum 3 years according to the request and the validation. Short-lived certificates are only acceptable when roll-over is automated.
The signing private key lifetime is seventy (70) percent of the verification key lifetime.
The certificate of the Rabobank CA is valid for twenty (20) years from date of issue.

4.5.3 Certificate Revocation List Management
The Rabobank CA produces an updated Certificate Revocation List (CRL) every six (6) hours.
The CRL is distributed to the appropriate Rabobank Directory System or http (OCSP) end-point. When certificates are revoked due to private key compromise, an updated CRL is generated immediately at that time and published to the Rabobank Directory System.

5 Certificate Usage Policy and Limitations

5.1 Rabobank Certificate Usage Policy Statement

X.509 public key certificates issued by the Rabobank are to be used solely for official business communications with Rabobank. Use of Rabobank issued certificates for other than official business communications with the Rabobank is expressly prohibited by the issuer. Any use of a Rabobank issued certificate for other than official business communications with the Rabobank is undertaken at the sole risk of the user.

5.2 Certificate Warning

As an official limitation on the authorized use of Rabobank CA issued certificates, the following statement is contained in all Rabobank CA issued certificates:

Browser certificate authorized by issuer solely for official business communication ***with Rabobank.***

This statement is part of the certificate data structure itself, and is digitally signed by the Rabobank CA digital signature key.