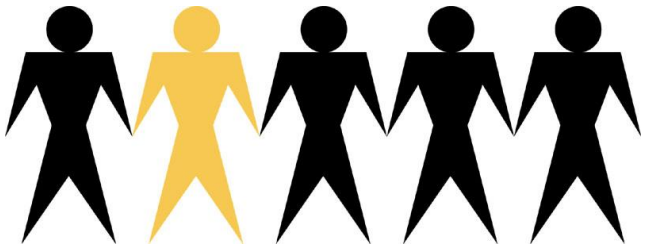
Volvo Group PKI Documentation

Volvo Group Certificate Practice Statement



Document name:	Volvo Group Certificate Policy Statement
Document Owner:	Volvo Group AB Corporate Process & IT
Issued by:	Volvo Group AB Certificate Center
Date:	2016-02-26
Version:	3.1
Replaces:	3.0
Approved:	Krister Samuelsson
OID	1.2.752.83.509.3.1.2

Document log

Date	Revision	Events
2003-12-04	1.00	First version
2003-12-19	1.01	CPS update and adjustment for creation of first Issuing CA
2004-04-19	1.02	CPS adjustments and updates for General Server Certificates
2004-06-23	1.03	Conformity review
2004-08-23	1.04	Adjustments, new certificate subject type, Application
2004-09-03	2.0	Final approved version, changes within 1.n.
2005-09-29	2.1	Adjustments, new certificate subject type, personal
2006-01-18	2.2	Adjustments, new certificate template, EFS
2013-01-15	3.0	Version three
2015-09-15	3.1	Removed obsolete information, updates of responsible and contact persons

Table of contents

Introduction

Advanced information technologies are increasingly being used to improve the effectiveness of business processes between partners. Business transactions are processed over public networks without the need for partners to be there 'in person'. This trend can be seen in the business-to business (B2B) and business-to-consumer (B2C) environment, and in the context of company-internal activities and communications.

The Volvo Group PKI (hereafter referred to as V-PKI) makes use of asymmetric cryptography to provide the basis for improved information security within the company. As part of this infrastructure, each user is assigned a pair of cryptographic keys. Together with encryption and a digital signature, this pair of keys will provide users and machines with the IT security required for these processes.

This document in most aspects follows the ETSI TS 102 042.

Identity of policies and documents in force
CP OID= 1.2.752.83.509.1.1.2
CVS OID= 1.2.752.83.509.2.1.2
CPS OID= 1.2.752.83.509.3.1.2
More information about these documents can be found in chapter 8 Identification of certificate policies, in this document.

1 Scope

This document describes the implementation of V-PKI. The intention is to allow employees and external users (business partners) to assess the reliability of the V-PKI (particularly the issued key material and certificates). In addition, specifications and information on the use of all elements of the V-PKI are given. The information given in this document is binding for the work of all parties involved in the V-PKI.

2 Reference

For information about CP and CVS, please see chapter 8 Identification of certificate policies, in this document.

3 Definitions

ADGOC (Active Directory Global Operation Co-ordination)	Manages, operates and coordinates the global Active Directory structure, covering Domain Controllers at Local sites and central servers.
Authentication	The process of verifying an identity claimed by or for a system entity.
CA-keys	CA's keys, where the private key is used to sign issued certificates and the public key to verify the validity of a certificate.
Catalogue	An electronic register that contains certificates, public keys and certificate revocation lists.
Catalogue Service	Provision of access to the catalogue mentioned above.
Certificate	An electronic certificate, stamped (signed) by the issuer, confirming that a public key belongs to a certain person or entity. Each certificate has a unique content of information and can always be identified.
Certificate Holder	A holder of a certificate approved and issued by the CA.
Certificate Policy (CP)	A named set of rules published by the certificate issuer that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certificate Revocation Check	Check made by the Relying Party to ensure that a certificate has not been revoked.

Certificate Revocation List (CRL)	Lists maintained by the CA containing the identities of all certificates that have been revoked.
Certificate Value Statement (CVS)	Rules establishing the minimum requirements for the issuing and use of electronic signatures within Volvo Group. The CVS, together with the CP, thus describes the requirements that the certification body has undertaken to fulfil.
Certification Authority (CA)	An entity responsible for issuing and signing certificates.
Certification Practice Statement (CPS)	A statement of the practices that a Certification Authority employs in issuing certificates, describing how the CP is interpreted in the context of the operating procedures of the CA.
Extended Key Usage (EKU)	Extended Key Usage indicates one or more purposes for which the certified public key may be used in.
Electronic Signature	Data in electronic form that are linked or logically connected to other electronic data and that are used to check that the content originates from the person who appear to be issuer, and that it has not been tampered with.
Encryption	Cryptographic transformation of data (called plaintext) into a form (called cipher text) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state.
FIPS 140	FIPS 140 is the (US) Federal Information Processing Standard that outlines security requirements for cryptographic modules. FIPS 140 is one of several cryptographic standards maintained by the Computer Security Division of NIST (National Institute for Standards and Technology).
HSM	A hardware security module (HSM) is a hardware encryption device that's connected to a server at the device level via PCI or SCSI interfaces.
Key Generation	The process that creates both public and private keys.

Local Registration Authority (LRA)	A local registration body of the CA. An entity that is responsible for identification and authentication of certificate subjects, but does not issue or sign certificates.
Private Key	The secret part of a pair of keys that is used for decryption or signature.
Public Key	The public part of a pair of keys that is used for encryption or verification.
Public Key Infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke Public Key Certificates based on public key Cryptography.
Registration Authority (RA)	A registration body of the CA. An entity that is responsible for identification and authentication of certificate subjects, but does not issue or sign certificates.
Relying Party	Person who receives and relies upon data that has been signed and/or encrypted by a certificate issued by Volvo Group.
Revocation	A marking that a certificate should no longer be considered reliable before its period of validity has expired.
Root	The CA that issues the first certificate in a certification chain. The root's public key must be known in advance by a certificate user in order to validate a certification chain. The root 's public key is made trustworthy by some mechanism other than a certificate, such as by secure physical distribution
Signature Verification Data	Data used to verify an electronic signature.
Subject	Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.
Subscriber	Entity subscribing with a Certification Authority on behalf of one or more subjects.
Volvo Corporate Directory	Volvo Corporate Directory is using Active Directory as an essential component for delivering operational services, e.g. directory services, within the Microsoft framework.

4 Contact Information

This CPS is registered, administered and updated by AB Volvo Corporate Process & IT
Questions concerning this CPS should be addressed to:

Volvo Group AB
Certificate Center
E-mail: certificatecenter@volvo.com

5 Publication

This CPS is made available at the address http://pki.volvo.com.

6 Applicability

This CPS applies to all Volvo Companies acting as a Certification Authority (CA) and/or Registration Authority (RA), any Certificate and Certificate Revocation List (CRL), directories and repositories used by Volvo Group and its affiliated companies, the CA and its operators, the Certificate Holders certified by the CA and the Relying Parties.

7 General concepts

7.1 Certification authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the certification authority. The certification authority has overall responsibility for the provision of the certification services in V-PKI. The root or issuing certification authority's key is used to sign the certificates and it is identified in the certificate as the issuer.

The certification authority may make use of other parties to provide parts of the certification service. However, the certification authority always maintains overall responsibility and ensures that the policy requirements identified in the present document are met. For example, a certification authority may sub-contract all the component services, including the certificate generation service. However, the key used to generate the certificates is identified as belonging to the CA, and the CA maintains overall responsibility for meeting the requirements defined in the CP, CVS and the present document.

7.2 Certification services

Corporate Process & IT provides, on behalf of Volvo Group, the Certification Authority services. The CA main responsibilities are

- Registration Service
- Certificate generation service
- Dissemination service
- Revocation management service
- Revocation service
- Management of V-PKI root keys, CA signing keys and the entire lifecycle of issued certificates.

The V-PKI enables a number of information security trust services. The services enabled by this V-PKI implementation can be categorized as:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation

There are a number of functions contributing to the certification services.

7.2.1 Registration Authority (RA) Services

The registration authority is an entity that is responsible for identification and authentication of certificate subjects. The RA determines whether the subject is eligible or not and sends approved applicants to the CA.

7.2.2 Local Registration Authority (LRA) Services

A local registration authority is doing the same activities as the RA. LRAs are used for practical reasons when e.g. there are big geographical distances involved or if the number of applicants is high.

7.2.3 Directory services

The directories contain public PKI data such as certificates and CRLs.

7.2.4 Support chain

The V-PKI solution will provide support according to the standard Volvo Support process.

- Service Desk
- 2nd Level Support
- 3rd Level Support

7.2.5 Key backup

All private CA keys are strongly encrypted and backed up and securely stored in three different locations. For subject type Personal encryption keys are backed up, no other subject type key are backed up.

7.3 Subscriber and subject

Certificates may be issued to a number of different subjects. The subject is the entity for which the certificate is issued, e.g. an individual, a machine or a job-role. For each subject, a subscriber, an identified person, must be responsible for the subject's certificate.

Two examples: For a personal certificate, the subscriber and the subject are identical; it is the person who will use the certificate. If the certificate is aimed to be used by a server, the server is the subject whereas a person responsible for the server is the subscriber.

The certificate subject types used are:

- Certificate subject type Personal
- Certificate subject type Role
- Certificate subject type Machine
- Certificate subject type Application

8 Services and functions

Volvo Group's PKI is used for the following services and functions.

Purpose	Service/Function	Description
SSL (Secure Sockets Layer)	Servers and clients	SSL is used to sign and encrypt traffic for network protocols, http and LDAP etc.
Smart card logon	End users and administrators	A smart card is used to provide strong authentication when required.
Remote access	Client VPN (Virtual Private Network)	Certificates are used for client authentication and enrollment of computers which use client VPN as remote access solution.
Radius traffic	Wireless access point	Certificates in conjunction with radius are used to provide centralized authentication, authorization, and accounting management for wireless access points.
Code signing	Developed scripts, programs, code	Code signing is used to secure that only approved code can be executed.
Document signing	Documents and files	Document signing is used when there is a need to prove that the content has not been tampered with or modified.
Secure e-mail	E-mail	Secure e-mail provides integrity and confidentiality protection of email communication . The messages can be signed and/or encrypted.

9 Identification of certificate policies

9.1 Overview

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements".
The policy requirements are defined in the CP and CVS documents in terms of certificate policies. Certificates issued in accordance with the V-PKI include a certificate policy identifier, which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.

Object Identifier (OID)
A specially formatted number, registered with an internationally recognized standards organization (SIS), and associated with a class of Certificates and a Certificate Policy, Certificate Value Statement and Certificate Practice Statement. X.509 V3 standard Certificates are used to list an Object Identifier.

9.2 Identification

The CP, CVS and CPS documents each have a unique identifier based on the Volvo Object Identifier (OID).
By including the object identifiers for the CPS in a certificate the CA claims conformance to the certificate policy.
The CPS must include references to the OID's of both the CP and CVS that govern the PKI.

9.2.1 Object identifier policy for V-PKI

Volvo Object Identifier base (OID) 1.2.752.83
1.2.752.83.509 Volvo Group Public Key Infrastructure (V-PKI)

1.2.752.83.509.1	Certificate Policy (CP)
1.2.752.83.509.2	Certificate Value Statement (CVS)
1.2.752.83.509.3	Certificate Practice Statement (CPS)
1.2.752.83.509.4	Certificate Class
1.2.752.83.509.5	Certificate Liability

CP, CVS and CPS
1.2.752.83.509.1.1.1
Explanation: The number is written in the form 1.2.752.83.509.A.B.C, where
A = Document type CP=1, CVS=2 and CPS=3
B = Document identifier
C = Version

The CPS OID shall be included in Certificate Policy field in certificate exclusive the version part. The version part shall be used in references from the CPS to CP and CVS.

Certificate Policy (CP)
For the participants of electronic communication to have confidence in the security of these cryptographic mechanisms they need to have confidence in the CA itself and in that the CA has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with public key crypto systems. The conditions under which the CA issues public key certificates and the legal responsibilities it takes when acting as a CA are formally regulated in the

Certificate Policy (CP). The CP thus states "what" is to be adhered to (the rules) and it can be regarded as an agreement between the CA and the Certificate Holders and the Relying Parties defining the responsibilities for each respective party as well as the applicability of a certificate to a particular community.

The CP states the conditions under which Volvo Group (and its affiliated companies) issues certificates, the "what" Volvo Group has to fulfil. It defines Volvo's legal responsibilities as a CA and should be regarded as an agreement.

Certificate Value Statement (CVS)
For the purpose of establishing the minimum requirements for the issuing and use of electronic certificates, the Volvo Group Certificate Value Statement (CVS) has been created. The CVS states the lowest level of administrative and security requirements that any CA acting on behalf of or on assignment from a Volvo Group company must fulfil. This means that irrespective if a Volvo Group company issues certificates itself, acting as a CA, or if this service is provided from an external CA/CSP all requirements stated in the CVS must be fulfilled. In case of obtaining certificates from an external CA/CSP the company must therefore assure that the provisions in the CVS are thoroughly discussed and regulated in the agreement between the CA/CSP and the Volvo Group company regarding the certificate service. Therefore the external CA/CSP's CP, CPS and any User Agreements also must be considered.

The CVS states the lowest level of administrative and security requirements that any CA acting on behalf of or on assignment from a Volvo Group company must fulfil.

Certification Practice Statement (CPS)
The way in which the CA fulfils its obligations as stated in the CP is described in the Certification Practice Statement (CPS). The CPS thus states "how" the CA adheres to the CP (i.e. a summary of the processes and procedures the CA will use in creating and maintaining certificates). The relationship between the CP and CPS is similar in nature to the relationship of other business policies that state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out. If a CA is issuing certificates against a number of CPs, then the CA's CPS (only one is necessary) will state how the CA implements the set of requirements (rules) to meet the needs of all the policies.

The CPS is a document, which specifies "how" the obligations in the CP and CVS are fulfilled.

Certificate class
1.2.752.83.509.4.1
Explanation: The number is written in the form 1.2.752.83.509.4.A, where
A= Certificate Class 1 to 4

1.2.752.83.509.4.1	Certificate Class 1
1.2.752.83.509.4.2	Certificate Class 2
1.2.752.83.509.4.3	Certificate Class 3
1.2.752.83.509.4.4	Certificate Class 4

Certificate class is used in qualified delegation to issuing CA's and in end-entity's certificates, when possible.

Certificate liability

1.2.752.83.509.5.1	No liability
1.2.752.83.509.5.2	Company low liability
1.2.752.83.509.5.3	Company high liability
1.2.752.83.509.5.4	Personal liability

Certificate liability OID is included in the EKU field. Default value is No liability.
Is only valid for electronic signatures use.

If no EKU OID for liability is included in certificate Volvo Group will not take any liability for the use of this certificate.

9.3 User community and applicability

The policies defined in the present document place no constraints on the user community and applicability of the certificate.

9.4 Conformance

9.4.1 Conformance claim

The CA shall only claim conformance to the present document as applied in the certificate policy identified in the certificate that it issues if:
a) It either claims conformance to the identified certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or
b) It has been assessed to be conformant to the identified certificate policy by a competent independent party.

10 Obligations and liability

10.1 Certification authority obligations

The V-PKI Root CA will:

- Comply with the CP, CVS and this CPS as published on the web site http://pki.volvo.com
- Provide infrastructure and certification services, including the establishment and operation of the web site for the operation of public PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own private key(s).
- Provide and validate application procedures for the various types of certificates that it makes publicly available. Depending on the certificate level, a request can be made in person by the applicant as well as be generated by a machine.
- Issue uniquely identifiable certificates in accordance with this CPS and fulfil its obligations presented herein.
- Notify applicants that certificates have been generated for them and how they may retrieve their certificates.
- Notify the applicant if Volvo Group is unable to validate the subscriber application according to this CPS.
- Upon receipt of a request of a RA operating within the Volvo Group network act promptly to issue a V-PKI certificate in accordance with this CPS.
- Upon receipt of a request for revocation from a RA operating within the Volvo Group network act promptly to revoke a V-PKI certificate in accordance with this CPS.
- Revoke certificates issued according to this CPS upon receipt of a valid request to revoke a certificate from a person authorized to request revocation.
- Provide support to subscribers and relying parties as described in this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Publish CRLs on a regular basis in accordance with this CPS. The frequency of publication of CRLs will vary according to the demands set out in the Certificate matrix.
- Notify relying parties of certificate revocation through published CRLs on the Volvo Enterprise Directory.
- Make a copy of this CPS and applicable policies available upon request.

10.2 Registration authority obligations

A V-PKI RA may be a person or a machine following a defined set of rules.
The RA will:

- Authenticate, according to the documented demands, entities requesting a certificate according to the procedures described in this document
- Determine if the subject, person or machine, has the right to have a V-PKI certificate
- Pass on validated certificate requests to V-PKI CA

10.3 Subscriber obligations

For any subject:

- An identified subscriber must be appointed

Any subscriber must:

- Make sure accurate and complete information is submitted to the CA in accordance with the requirements of this document, particularly with regards to registration
- Take responsibility for recovery arrangements in case of loss of private key
- Keep the private key safe and protected
- Use the certificates for permitted purposes only

Notify the V-PKI CA/RA:

- In case of possible private key compromise, key destruction or loss
- In case control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or
- If the certificate is no longer required for its original purpose
- If the distinguished name of the subject changes,
- If a subject is no longer trusted
- If operations are discontinued

Unless otherwise stated in this CPS, all subscribers are responsible for:

- Having knowledge of and if necessary seek training on the using of certificates and public key encryption.
- Generating securely their private key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with Certificate Center including certificate application.
- Ensuring that the public key submitted to Certificate Center corresponds to the private key issued.
- Ensuring that the public key submitted to Certificate Center is the correct one.
- Generating a new, secure key pair to be used in association with a certificate upon request from Certificate Center.
- Reading, understanding and agreeing with all terms and conditions in this CPS and other policies published on the Volvo Corporate Network / Intranet at the address (http://pki.volvo.com).
- Refraining from tampering with a V-PKI certificate.
- Using V-PKI certificates for legal and authorized purposes in accordance with the CP, CVS and this CPS.
- Notifying V-PKI CA or a V-PKI RA of any changes in the information submitted or of any fact that affects the integrity of the private key.
- Ceasing the use of a V-PKI certificate if any featured information becomes invalid.
- Ceasing the use of a V-PKI certificate when it becomes invalid.
- Refraining from using the subscriber's private key corresponding to the public key in a V-PKI issued certificate under its name to have other certificates issued.
- Using a V-PKI certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key and taking measures for the appropriate protection of the private key.
- Complying with any restrictions in the usage of the key or certificates.
- Using secure devices and products that provide appropriate protection to their keys.
- Any acts and omissions of subscribers' partners and agents that the subscribers use to generate, retain, escrow, destroy or otherwise handle any private keys.
- Refraining from submitting to V-PKI or to any Volvo Group Directory any material that contains statements or other information that violate any law or the rights of any party.

- Requesting the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a V-PKI certificate.
- Appropriately supervising agents or partners that apply for or use a V-PKI certificate on behalf of the subscriber.

Indemnity
The subscriber agrees to indemnify Volvo Group for any acts or omissions resulting in liability, any loss or damage and any suits and expenses of any kind, including reasonable attorneys' fees that Volvo Group may incur as a result of:

- Any false or misrepresented data supplied by the subscriber or its agent(s).
- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Volvo Group, or any person receiving or relying on the certificate.
- Failure to protect the subscriber's private key, to use a trustworthy system as required, or to take precautions necessary to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the subscriber's private key or to attend to the integrity of the V-PKI Root.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, export, import or domestic usage of cryptographic products, viruses, accessing computer systems etc.

10.4 Information for relaying parties

- Read and accept the policies and procedures published in this document
- Follow the instruction concerning CRL checking requirements for relaying parties
- Use the certificates for permitted purposes only

10.5 Liability

For detailed liability information, please refer to CVS OID=1.2.752.83.509.2.1.2 and CP OID=1.2.752.83.509.1.1.2

11 Requirements on CA practice

11.1 Public key infrastructure - Key management life cycle

All key management activities will be carried out by personnel in trusted roles. The number of personnel authorized to carry out this function will be kept to a minimum and be consistent with the CA's practices.

11.1.1 Certification authority key generation

The CA shall ensure that CA keys are generated in controlled circumstances. Certification authority key generation will be undertaken in a physically secured environment. CA key generation will be carried out within an HSM-device, which meets the requirements identified in FIPS PUB 140-2 level 3.

The *x of y* functionality has been implemented for this solution. This means that a minimum number of role holders ("x") must be present before any action can be taken with the module. The administration role holders are identified with strong authentication (2-factor authentication).

	Root CA	Issuing CA 1	Issuing CA 2
Administrator Role Holder	3/6	3/6	3/6
Operator Role Holder	3/6	1/4	1/4

The “x” is less than “y” in order to ensure that a card loss or failure does not prevent a quorum being maintained.

11.1.2 Certification authority key storage, backup and recovery

The CA shall ensure that CA private keys remain confidential and maintain their integrity.

The CA’s private key will be backed up in multiple copies and stored on several controlled secure places both on and off site. The CA’s private key will never leave the HSM unencrypted.

The CA will be recovered within the expiration time of the CRL.

11.1.3 Certification authority public key distribution

The CA certificates will be published in the Volvo’s Enterprise LDAP directory and at http://pki.volvo.com/pki The CA certificates will also be distributed to the managed clients through built in functions in our client environment.

11.1.4 Key escrow

Key Escrow is not supported.

11.1.5 Certification authority key usage

V-PKI Root CA Private Keys are used solely for the purpose of generating and signing certificates within physically and logically secure premises, and for the purpose of signing revocation information. Other usage is prohibited.

11.1.6 End of CA key life cycle

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle. All copies of the CA private signing keys will be made unusable in a way that the private keys cannot be retrieved. The CA certificate will be kept available and published as specified as long as it is needed.

11.1.7 Life cycle management of cryptographic hardware used to sign certificates.

The CA will ensure the security of cryptographic device throughout its lifecycle. All cryptographic hardware used will be physically protected and an audit log will be kept for all access to the hardware, from delivery to our premises to the decommission of the device. Before the cryptographic hardware will be decommissioned it will be erased of all information through a reset.

11.1.8 CA provided subject key management services

The CA does not generate any subject keys in this solution.

11.1.9 Secure user device preparation

Hardware security tokens are not used in this solution.

11.1.10 Characteristics of Certificates, Keys

V-PKI Certificate classes

Certificate Class	Requirements for authen-tication	Requirements for private key storage	OID
Class 1	Basic validation	No requirement	1.2.752.83.509.4.1
Class 2	Subscriber identified by ID and password against approved directory	Encrypted on disk	1.2.752.83.509.4.2
Class 3	Same as for Class 2 with addition of out of bound	Encrypted on disk with approved method	1.2.752.83.509.4.3
Class 4	Have to appear in person and validate his identity	FIPS validated hardware device certified to at least FIPS 140-1 level 2	1.2.752.83.509.4.4

For a certificate to fulfil a certain level it has to fulfil all requirements specified for this level or higher. In this phase only Class 2 is used.

Class 1: Basic validation of the applicant's identity. Primarily for non-Volvo employees.

Class 2: Subscriber identified by user ID and password against approved directory, e.g. The Volvo Corporate Directory. Auto enrolment is allowed if the requirement for authentication is fulfilled.

Class 3: Applicant identified by strong authentication or similar method as in Class 2 and comple-mented with a separate channel method as PIN letter distributed through internal mail, or picked up at designated place after proper identification.

Class 4: Applicant must appear in person to appointed LRA and be identified by Volvo Group issued identity card or other approved method.

11.2 Public key infrastructure - Certificate management life cycle

V-PKI Certificate Lifecycle Plan

Certificate	Key length	Lifetime	Private key renewal
Offline Root CA	2048	20 years	Renew every 10 years with new key
CLASS 2 Issuing CA	2048	10 years	Renew every 5 years with new key

CLASS 2 Issuing CA	2048	10 years	Renew every 5 years with new key

11.2.1 Subject registration

The CA will ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that subscriber certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

The requirement differs between different Certificate classes and different kinds of subjects as specified in the following section

Class 1, 3, and 4 are not in use.

Class 2

Certificate subject type Personal:

The subject orders access a certificate Template via a web application. An approval, from a manager in the subject's organization, is often required. The subject is granted enrolment rights via security group membership in AD. The enrolment can either be manual or auto.

Certificate subject type Role:

The subscriber requests the enrolment of the subject to the appointed RA or LRA.
The RA or LRA validates the subscriber and the subject and grants the subject the right to have a certificate.

Certificate subject type Machine and Application:

The subscriber requests the enrolment of the subject to the appointed RA. The RA validates the subscriber and the subject and grants the subject the right to have a certificate.
Auto enrolment is possible for client and server certificates that are issued to the computer-name or fully qualified domain name (FQDN).
For a generic server or application certificate the subscriber has to order a certificate from a web application (Certificate Lifecycle Management tool).

11.2.2 Certificate renewal, rekey and update

The CA must ensure that requests for certificates issued to a subject who has previously registered with the same CA are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes.

The requirement differs between different Certificate classes and different kinds of subjects as specified in the following section

Class 1, 3, and 4 are not in use.

Class 2

Certificate subject type Personal:

The subject makes a request for renewal, rekey or update to the CA. For a manual renewal, a notification via email will be sent to the subscriber informing about the certificate expiration, the subject then makes a request via a web application. In other cases the renewal is automatic with user interaction.

Certificate subject type Role, Machine and application:
The subject or subscriber makes a request for renewal to the CA.

11.2.3 Certificate generation

The CA will ensure that it issues certificates securely to maintain their authenticity.

Class 1, 3, and 4 are not in use.

Class 2
The subscriber always identified against a managed directory.

Certificate subject type Personal:
The certificate will be deployed directly to the authenticated subscriber either automatically on via a web application.

Certificate subject type Role, Machine and application:
The certificate will be sent to the subscriber's functional mailbox specified during the order process.

11.2.4 Key archiving and key recovery

All events involved in the archiving process are being logged. The subject receives a certificate signed by the issuing CA, the certificate and the associated private key are archived in the CA database.

Class 1, 3, and 4 are not in use.

Class 2
Certificate subject type Personal:
The subject makes a request for key recovery to the CA. The subject makes this request via a web application.

If ***a*** company needs a key recovery of a subject's private key to the request shall be sent to the RA. This procedure must follow Volvo Groups' instructions for accessing ***personal*** data.

Certificate subject type Role, Machine and application:
NA

11.2.5 Dissemination of terms and conditions

Information about terms and conditions for the V-PKI CA is to be found at the official website, http://pki.volvo.com.

11.2.6 Certificate dissemination

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties.

11.2.7 Certificate revocation and suspension

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.

Rules for revocation
Class 1, 3, and 4 are not in use.

Class 2
Certificate subject type Personal, Role, Machine and Application:
The subscriber or a manager from the subscriber's organization must approve revocation.

CRL publication
The CRLs will be published through the Volvo Enterprise Directory and on the web site http://pki.volvo.com.

Root CA
Maximum CRL Lifetime 12 months
Renew every 6 months

Issuing CA 1
Maximum CRL Lifetime 14 days
Renew every 7 days
New CRL Issued every day and on demand if/when necessary.

Issuing CA2
Maximum CRL Lifetime 14 days
Renew every 7 days
New CRL Issued every day and on demand if/when necessary.

11.3 CA management and operation

11.3.1 Security management

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

11.3.2 Asset classification and management

The CA shall ensure that its assets and information receive an appropriate level of protection.

11.3.3 Personnel security

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.

11.3.4 Physical and environmental security

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized. This is seen to through adherence to Volvo Group's "**DCS, Data Center Setup reference manual**". Furthermore the CA is secured through a reinforced and tamperproof server cabinet.

11.3.5 Operations management

Volvo Group undertakes certain operational controls including organizational, human resources, and other management-related controls commensurate with the level of service it offers and the specific requirements of individual contracting parties.

Such controls include:

- Specified and documented (trusted) roles and responsibilities.
- Specified and documented job descriptions (ref: Volvo Group Management System -VGMS).
- Appropriate measures for authentication of CA staff (Volvo ID-card).
- Employee training and awareness.

11.3.6 System access management

- The CA shall ensure that CA system access is limited to properly authorized individuals.
- The Root CA system is secured by never having a network connection.
- All CA system operations are always carried out by at least two authorized CA personnel together.
- All access to the CA system is logged continuously in dual logs

11.3.7 Trustworthy systems deployment and maintenance

- The CA shall use trustworthy systems and products that are protected against modification.
- The root CA system is deployed through a well-documented Key signing ceremony.
- The issuing CA's are secured via locked down configuration.
- All Software used is validated and signed by each software vendor
- All cryptographic operations take place within a FIPS 140-2 level 3 validated HSM.
- The CA system is secured and tamper resistant by the use of seals and labels in several tiers.

11.3.8 Business continuity management and incident handling

Based on risk analyses, the most critical scenarios, e.g. a compromise of the CA or a technical breakdown, will be accounted for in Business Continuity Plans as well as Disaster Recovery Plans. The plan as well as the scenarios will be regularly revised.

In the case of a critical scenario a complete recovery of the entire CA system will be done within one week. Such a recovery will be possible through our Operation Guide document and this CPS.

11.3.9 CA termination

In this context, cessation of V-PKI's CA business activities means that all services associated with the CA business activities cease.

Before Volvo Group may end its CA business activities; Volvo Group will take the following measures:

- Inform all Certificate Holders
- Publish information about the cessation of the CA business activities on Volvo Group's web-site, if possible, three months in advance
- End the service for certificate revocation checking
- End all rights for sub-suppliers to act in the name of Volvo Group
- Ensure access to archived material.

11.3.10 Compliance with legal requirements

Volvo Group complies with applicable laws and regulations in each country or region it carries out business. Information regarding Volvo Group's legal responsibilities and liability when acting as a CA can be found in:

- CP OID= 1.2.752.83.509.1.1.2 and
- CVS OID= 1.2.752.83.509.2.1.2

11.3.11 Recording of information concerning certificates

Record retention is performed using secure mechanisms, primarily for the purpose of complying with applicable national and international legal demands and for the purpose of providing admissible evidence of certification for legal proceedings. In doing so, V-PKI CA ensures that all relevant information concerning a certificate is recorded and retained according to management, legal, audit, tax or other compliance requirements.

11.4 Organizational

The following chapter describes the PKI organization with roles and their responsibilities. Contact persons and addresses for all involved individuals can be found in appendix "PKI Services and Contact Persons".

11.4.1 General

General

Personnel involved in V-PKI should:

- Be trusted personnel, i.e. have the necessary education and understanding, in order to be able to perform their duties in an impeccable way.
- Be aware of the risks and security arrangements that can affect the V-PKI operation.

The V-PKI organization will have defined deputies appointed as backup for each role.
The V-PKI organization will utilize separation of duties on all its roles.
The V-PKI organization will operate under clearly defined and documented operational procedures.

11.4.2 V-PKI Owner and Certification Authority (CA)

AB Volvo Corporate Process & IT is the V-PKI owner and the Certification Authority (CA) of Volvo Group.

Overall PKI Owner Responsibilities

- The Volvo Group PKI Owner has the responsibility to approve change requests for the PKI infrastructure, including decisions to set up or terminate Issuing CA's.

Overall CA Responsibilities

- The Volvo Group Root CA has the obligation, and only on request from the PKI Owner the right, to set up or terminate Issuing CA's.

11.4.3 PKI Security Officer

PKI owner appoints the PKI Security Officer.

Overall Security Responsibilities

- The Security Officer shall make sure that Volvo Group's general security policies are followed in all parts of the PKI operation.
- The Security Officer is the contact person towards the CA in all security issues.

Reviews and Monitoring

- Audits of the V-PKI operation shall be made at least once a year. The V-PKI operation shall also be audited upon a major change.
- The CA operation shall be audited at least once a year. The CA operation shall also be audited upon a major change.
- Security deficiencies are reported to the PKI Service Manager.

11.4.4 PKI Service Manager

The Certificate Center Line Manager is the PKI Service Manager. The PKI Service Manager has the overall responsibility of the operation.

Included responsibilities are:

- Manage changes and enhancements in V-PKI, as agreed with the V-PKI owner.
- Coordination and integration of other effected systems and other similar services.
- Cessation of V-PKI operation.
- Coordination of internal policies and legal issues.
- Takes authorization decisions.
- Cost level of the services for both internal and external use.

11.4.5 CA Operation

Volvo Group ADGOC (Active Directory Global Operation Co-ordination) manages, administers and handles the daily operation and maintenance of V-PKI.
Administrator role holders are required for initial set up of CA and disaster recovery actions. Operation role holders are required for maintenance and operation actions.

11.4.6 Registration Authority (RA)

Volvo Group Certificate Center manages and administers the RA operation of V-PKI.

The RA service is divided in services managed by a number of Local Registration Authorities (LRA) and the Registration Authority (RA).

The registration authority is an entity that is responsible for identification and authentication of certificate subscribers and subjects. The RA determines whether the subscriber and subject is eligible or not and sends approved applications to the CA.

A local registration authority (LRA) is doing the same activities as the RA. LRAs are used for practical reasons when e.g. there are big geographical distances involved or if the number of applicants is high.

11.4.7 Support Chain

The V-PKI solution will have support according to the standard Volvo Support process.

Service Desk

The Service Desk should be able to manage questions as:

- Who to turn to regarding general V-PKI issues, i.e. 2nd Level Support, RA or the PKI Security Officer.
- Where documents can be found concerning V-PKI.

- Information and escalation of software problems to second level support.

2nd Level Support
Volvo Certificate Center and ADGOC act as 2nd Level Support.

2nd Level Support should be able to manage issues as:

- Hold short V-PKI training sessions to Service Desk staff, RA and end-users.
- Error handling and change management such as installation of critical system related patches.
- Information and escalation of software problems to third level support and vendors.
- Technical support such as suggestions about tuning and solutions.
- Recommendations about available system upgrades.

3rd Level Support

3rd Level Support service has knowledge of all V-PKI components.

3rd Level Support is an external service, available according to a service agreement.

12 Framework for the definition of other certificate policies

Not in use.

12.1 Certificate policy management

Not in use.

12.2 Additional

Not in use.

12.3 Conformance

Not in use.

13 Appendix

13.1 PKI Services and Contact Persons

Volvo Group PKI organization

PKI roles & services	Responsible	Contact
PKI Owner & Certification Authority (CA)	AB Volvo Corporate Process & IT is the Volvo PKI owner and the Certification Authority (CA) of Volvo.	Krister Samuelsson krister.samuelsson@volvo.com IT Security & Compliance
PKI Service Manager	Certificate Center Line Manager	Stefan Oscarsson stefan.oscarsson@volvo.com Identity and Access Management
PKI Security Officer	AB Volvo Corporate Process & IT appoints the PKI Security Officer.	Anders Dovblad anders.dovblad@volvo.com Identity and Access Management
CA Operation	Volvo Group ADGOC manages, administers and handles the daily operation and maintenance of Volvo PKI.	ADGOC Team adgoc@volvo.com
Registration Authority (RA)	Volvo Group Certificate Center manages and administers the RA operation of Volvo PKI.	Certificate Center certificatecenter@volvo.com
Support Chain	The V-PKI solution will have support according to the standard process. 1. Service Desk 2. 2nd Level Support (Certificate Center and ADGOC) 3. 3rd Level Support (nCipher, Microsoft)	

Volvo Group PKI Organization