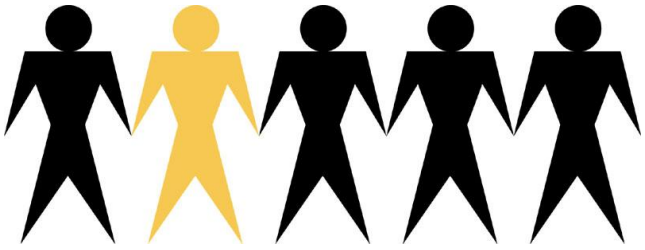
Volvo Group PKI Documentation

Volvo Group Certificate Policy



Document name:	Volvo Group Certificate Policy
Document Owner:	AB Volvo Corporate Process & IT
Issued by:	Volvo IT Certificate Center
Date:	2013-01-15
Version:	3.0
Replaces:	2.0
Approved:	Kerstin Löfstedt
OID	1.2.752.83.509.1.1.2

Document log

Date	Revision	Events
2003-12-12	1.0	First version
2003-12-19	1.01	Approved by Kerstin Löfstedt
2004-04-19	1.02	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.
2013-01-15	3.0	Version three

Table of contents

1 Volvo Group PKI – Policies and documentation

1.1 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

1.2 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 has to fulfil. It defines Volvo's legal responsibilities as a CA and should be regarded as an agreement.

1.3 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 company must fulfil. This means that irrespective if a Volvo 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 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 company must fulfil.

1.4 Certification Practice Statement (CPS)

The way in which the CA fulfils its obligations as stated in the CP is outlined 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 CP's, 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 an internal document, which specifies ***"how"*** the obligations in the CP and CVS are fulfilled.

2 General

This Certificate Policy (CP), together with the Volvo Group Certificate Value Statement (CVS), specifies the requirements under which Volvo Group offers services for issuing certificates. It shall thus be deemed to constitute the overall agreement to which the Certificate Holders and the Relying Parties who use the provided services must adhere to.

The rights of the Certificate Holders and the Relying Parties to use the services are regulated by this CP as well as by special agreements. Such special agreements take precedence over this CP. This CP applies only to Volvo Group's role in issuing certificates and in providing revocation functions for such certificates (CA business activity).

3 Applicability and Contract Parties

3.1 Applicability and Identification

This CP is applicable to the following electronic signature certificates:

The types of certificates governed by this CP shall be listed in the following. As new certificate types are implemented at Volvo, the CP must accordingly be modified. Certificate types presently not in use are indicated with “not in use”.

3.1.1 Personal Liability Certificate

NOT IN USE

3.1.2 Company Liability High Certificate

NOT IN USE

3.1.3 Company Liability Low Certificate

NOT IN USE

3.1.4 Non-Liability Certificate

Non-Liability Certificate, in accordance with the requirements and conditions set out in the Volvo Group Certificate Value Statement (CVS) regarding such certificates.

Certificate Policy Name:	This CP
Object Identifier:	CP OID= 1.2.752.83.509.1.1.2

Volvo Group accepts no financial liability for the above mentioned certificate type.

3.2 The Parties

This CP applies to Volvo Group, its subsidiary and affiliated companies and to sub-suppliers engaged by Volvo Group to issue and use certificates or to provide related services for Revocation and Revocation Checking, the Certificate Holders and the Relying Parties, which all are parties to the overall agreement.

4 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.
Time-stamping Authority (TSA)	Authority which issues time-stamp tokens.
Time-stamp policy	Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements
Time-stamp token	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time .
TSA system	Composition of IT products and components organized to support the provision of time-stamp

	services
Time-stamping unit	Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.
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.

5 Contact Information

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

Volvo Information Technology
Certificate Center
E-mail certificatecenter@volvo.com

6 Publication

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

7 Responsibilities and Undertakings

7.1 Certificate Authority

Volvo Group warrants to the agreement parties that, within the scope of its business activity as a Certificate Authority (CA), it will issue certificates and provide Revocation Functions for them, and fully meet all responsibilities as set out in this CP, the CVS and in any other special agreement entered into between and by the Certificate Holders and Volvo Group, its subsidiary or affiliated companies.

Volvo Group has access to sufficient resources in the form of its own means together with insurance to be able to fulfil its obligations as stated in this CP, the CVS and any other special agreements.

7.1.1 CA´s Private Keys

Volvo Group warrants that its CA's Private Keys are used solely for the purpose of generating certificates within physically and logically secure premises, and for the purpose of signing revocation information.

Volvo Group is obliged to take the measures necessary to protect its CA's private keys and ensure that these are not used after the expiration of the respective certificates period of validity. If unauthorized access to Volvo Group CA's private keys is suspected, Volvo Group will undertake following measures:

1. All Certificate Holders to whom certificates have been awarded will be informed.

2. The Certificate Revocation Check Service relating to the keys to which an unauthorized access is suspected ceases immediately.

3. The certificates that have been generated using the keys to which an unauthorized access is suspected will be revoked as soon as reasonably practicable.

7.1.2 Publication of Certificate Information

Issued certificates are published in the Volvo Enterprise directory according to current standards. The Catalogue Service is available to the agreement parties thru authenticated LDAP access to the Enterprise directory.

Volvo Group continuously generates lists of revoked certificates (Certificate Revocation Lists), the most current list being made publicly available in the Volvo Enterprise directory and on the website http://pki.volvo.com. On-line control of the status of revocation is provided by the Catalogue Service and from the website 365 days a year 7 days a week 24 hours a day except in the event of system failure or other reasons beyond the control of Volvo Group or activities related to normal maintenance. Information on revoked certificates is stored in the Certificate Revocation List (CRL).

7.1.3 Volvo Group Root CA obligations

The Volvo Group Root CA has the obligation, and only on request and approval from the PKI owner the right, to set up or terminate sub CAs.

7.2 Registration Authority

RA's will carry out its service in accordance with the conditions and obligations required by this CP, the CVS, the CA's Certification Practice Statement (CPS), the Volvo Group Security Policy and any other relevant Volvo Group Policies, Directives and Standards.

7.3 Certificate Holders

The Certificate Holder is obliged to retain control of his/her private key and take necessary precautions to prevent its loss, disclosure to any other party, modification or any other unauthorised use. The certificate holder is obliged to revoke his/her certificate whenever reasons for revocation occur.

7.4 Relying Parties

It is the responsibility of the Relying Party to verify the status of the certificate; either by checking the most recently published CRL, in order to ensure that the relevant certificate is currently valid.

The Relying Party shall ensure either that the certificate is checked against a CRL that:

1. represents the most recent, current revocation information available for the certificate in question,
2. is valid, i.e. has not expired, and
3. originates from a valid source.

If the CA provides online certificate status service, the Relying Party must ensure that the service used is the current one and that it is verified to originate from a valid source.

It is the Relying Party's responsibility to check the certificate status prior to accepting the validity of an electronic signature or certificate.

If the latest CRL cannot be obtained from the directory, due to system failure or service, no certificates should be accepted if the validity period of the last retrieved CRL has expired. Any acceptance of a certificate after this expiration is done at the Relying Party's own risk. The same applies to the situation where the Relying Party uses the CA's online certificate status service, and this cannot be accessed due to system failure or service. Any acceptance of a certificate when online certificate status service cannot be obtained is done at the relying party's own risk.

It is the responsibility of the Relying Party to note the limitations to the use of the certificate that are notified to the Relying Party either in the certificate itself or in the conditions and requirements set out in this CP or in any other special agreements.

It is the responsibility of the Relying Party to ensure that the certificate fulfils the Relying Party's requirements regarding security and that the certificate is suitable for the purpose in question.

8 Limitation of Liability

The Limitation of Liability will be defined when other certificate types are in use. Before that Volvo Group takes no responsibility whatsoever for the unauthorized use of private keys and certificates.

This CP does not protect against fraud and misuse of the Certificate Holder's private key.

9 Processing of Personal Data

For the purpose of providing and administrating the service, Volvo Group will process the personal data of the Certificate Holders in accordance with current legislation. Personal data that are passed on to Volvo Group in order for Volvo Group to issue certificates may thus be registered in commonly available catalogues and thereby be made available within and outside EU Member States or countries affiliated to the European Economic Area (EEA).

All processing of personal data will be performed in accordance with the provisions set out by local legislation.

10 Intellectual Property Rights and Ownership Rights

Volvo Group owns all intellectual property rights and ownership rights to all information, technical solutions and equipment provided by Volvo Group in connection with the service and no other person or entity shall own the right to use commercially, copy or otherwise process or distribute information regarding the service unless prior written consent has been granted by Volvo Group in each specific case.

Copyright Owners that supply Volvo Group with Material necessary for Volvo Group to provide its service under this CP guarantee that they own or otherwise control the Material and that copyright owners of any third party material has granted permission, without

limitation, to all the rights necessary for the Copyright Owners to provide the Material to Volvo Group.

11 Confidential Information

Information that is not expressly exempted or otherwise defined as public in this CP or any specific agreements shall be treated as confidential and may not be revealed without prior written approval from the parties affected unless required by law, constitution or decision of an authority. Issued certificates, CRL's, public keys as well as conditions for Certificate Holders shall never be regarded as confidential.

12 Document Alterations

Alterations to this CP that only constitute modifications of the language and rearrangements that do not affect the actual contents can be made without notice.

Other changes can be made ten days after notice has been given to the document owner.

13 Cessation of the business as CA

In this context, cessation of Volvo Group'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 website, 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, and
- Ensure access to archived material.

14 Interpretation and Enforcement

Any dispute, controversy or claim arising out of or in connection with this CP, or the breach, termination or invalidity thereof, shall be governed by Swedish law and finally settled by arbitration in accordance with the Rules for Expedited Arbitrations of the Arbitration Institute of the Stockholm Chamber of Commerce.

If any term, condition or provision in this CP is determined to be unlawful, invalid, void or for any other reason unenforceable, the validity and enforceability of the remaining terms, conditions and provisions shall not in any way be affected or impaired thereby.

15 Period of Validity

This CP is valid from and including 19th December 2003 until further notice.