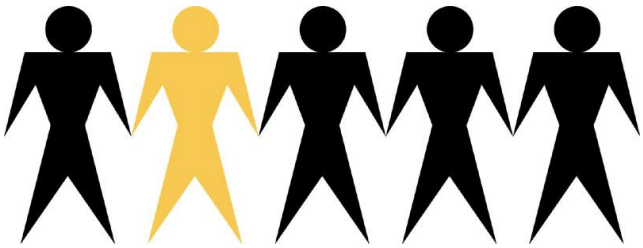
Volvo Group PKI Documentation

Volvo Group Certificate Value Statement



Document name:	Volvo Group Certificate Value State-
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	1.2.752.83.509.2.1.2

Document log

Date	Revision.	Events
2003-12-04	1.00	First Version, Approved by Kerstin Löfstedt
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 Introduction

2.1 Overview

The purpose of this Certificate Value Statement (CVS) is to establish the minimum requirements for the issuing and use of electronic signatures within Volvo Group. This CVS thus states the lowest level of administrative and security requirements in order to obtain electronic signatures of different legal and organizational value.

The certificates issued in accordance with this CVS are typically suitable for verifying the identity of individuals/entities and the authenticity of digital documents and other information objects in connection with information services. Certificates issued in accordance with this CVS may be suitable for a wide range of applications, primarily focusing on the following main classes of security services:

- Non-repudiation: the party relying on the certificate can be confident that their counterpart cannot deny an exchange of information.
- Authentication (including authentication of subscribers identity and message integrity).
- Confidentiality: unauthorized persons cannot gain access to confidential information or classified systems.

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.
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.

4 Contact Information

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

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

5 Publication

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

6 Applicability

This CVS 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 Levels of Liability

Certificates within Volvo Group are, for the time being, divided into four (4) levels of liability. These levels are:

- Personal Liability
- Company Liability High
- Company Liability Low
- Non-Liability

In order for Volvo Group to take legal responsibility for issued certificates, and their use within and outside the organization, the organizational, legal, administrative and security requirements stated in this document must be fulfilled.

7.1 Personal Liability

[NOT INCLUDED IN THIS VERSION]

7.2 Company Liability High

[NOT INCLUDED IN THIS VERSION]

7.3 Company Liability Low

[NOT INCLUDED IN THIS VERSION]

7.4 Non-Liability

Summary

Non-Liability certificates are used when there are requirements for non-legal bindings or requirements for no liability for the: issuer, subject or any other part using the certificate type.

The Non-Liability certificates are not creating any legal binding signatures. Volvo Group accepts therefore no financial or other type of liability for the mentioned certificate type.

7.4.1 Legal and Organizational Requirements

Not applicable.

7.4.1.1 Volvo Group

Not applicable.

7.4.1.2 EU

Not applicable.

7.4.1.3 USA

Not applicable.

7.4.1.4 Other Regions/Countries

Not applicable.

8 Interpretation and Enforcement

Various laws and regulations will apply, depending upon the jurisdiction(s) in which certificates are issued and used. It is the responsibility of the entities concerned to ensure that all applicable laws and regulations are followed.

Precise dispute resolution procedures shall be stated in the respective CA's Certificate Policy and/or any other agreements concerning the certificates.