

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

Ericsson Group Certificate Value Statement

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

Contents

1	Ericsson Certificate Value Statement	3
2	Introduction	3
2.1	Overview	3
3	Contact information	3
3.1	Specification administration organization	3
4	Publication	3
4.1	Revisions	4
4.1.1	Revisions	4
5	Applicability	4
6	Types of electronic signatures	4
6.1	Personal Liability	4
6.2	Company Liability High	4
6.2.1	Summary	4
6.2.2	Legal and organizational requirements	5
6.2.3	Certification Authority obligations	6
6.2.4	Registration Authority obligations	8
6.2.5	Requesting party obligations	9
6.2.6	Relying party obligations	9
6.2.7	Certificate holder obligations	10
6.2.8	Certificate Profile	11
6.2.9	Requirements for issuing certificates	11
6.2.10	Certificate usage	11
6.2.11	Ownership rights	11
6.2.12	Revocation	11
6.3	Company Liability Low	12
6.3.1	Summary	12
6.3.2	Legal and organizational requirements	12
6.3.3	Certification Authority obligations	13
6.3.4	Registration Authority obligations	15
6.3.5	Requesting party obligations	16
6.3.6	Relying party obligations	17
6.3.7	Certificate holder obligations	17
6.3.8	Certificate Profile	18
6.3.9	Requirements for issuing certificates	18
6.3.10	Certificate usage	19
6.3.11	Ownership rights	19
6.3.12	Revocation	19
6.4	Non-Liability	19
7	Interpretation and enforcement	20
8	Definitions	21

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

1 Ericsson Certificate Value Statement

This Certificate Value Statement stipulates the requirements that must be fulfilled when issuing certificates for the use of electronic signatures within Ericsson.

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 Ericsson. This CVS thus states the lowest level of administrative and security requirements in order to obtain digital signatures of different legal and organizational value.

The certificates issued in accordance with this CVS are typically suitable for verifying the identity of 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 Contact information

3.1 Specification administration organization

This Certificate Value Statement is registered by, administered and updated by LME/DA (Ericsson Group Security).

Questions concerning this policy should be addressed to:

Ericsson Group
LME/DA
VP Group Security, Hans Dahlquist
SE-164 83 Stockholm

4 Publication

This CVS is made available on Ericsson's web site and can be obtained in electronic form.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

4.1 Revisions

4.1.1 Revisions

Rev A	Checked by Gunilla Modén, Vice President Legal Affairs	Approver: Hans Dahlquist, Vice President Security & Risk Management

5 Applicability

This Certificate Value Statement (CVS) applies to all Ericsson companies acting as a Certification Authority (CA) and/or Registration Authority (RA), any certificate and certificate revocation list (CRL) directories and repositories used by Ericsson, the CA and its operators, the Certificate holders certified by the CA and the Relying parties.

6 Types of electronic signatures

Within Ericsson four different types of electronic signatures have, for the time being, been identified. These electronic signatures may be exercised by using one of the following types of certificates:

- Personal Liability
- Company Liability High
- Company Liability Low, and
- Non-liability.

In order for Ericsson 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.

6.1 Personal Liability

Currently not accepted.

6.2 Company Liability High

6.2.1 Summary

“Company Liability High”-certificates are aimed to be used in order to obtain legally binding electronic signatures on a company level and to meet legal requirements for non-repudiation with regards to originator of an electronic record. Any certificate issued as a “Company Liability High”-certificate must therefore comply with relevant current legislation.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

In order for Ericsson 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.

6.2.2 Legal and organizational requirements

6.2.2.1 Ericsson

The Ericsson requirements on a "Company Liability High"-certificate are that the electronic signatures one may create by using the certificates are to be legally binding within all the regions where Ericsson are represented. Any electronic record secured with such a certificate should meet the standards required for non-repudiation with regards to the originator of the record.

Furthermore the certificates shall comply with the Council Directive 2001/115/EC of 20 December 2001, amending Directive 77/388/EEC, with a view to simplifying, modernizing and harmonizing the conditions laid down for invoicing in respect of value added tax. This means that a "Company Liability High"-certificate at least shall fulfill the requirements for an "advanced electronic signature" as set out in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

6.2.2.2 EU

When it comes to the legal effect of electronic signatures the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures state that the Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

- satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
- are admissible as evidence in legal proceedings.

The Member States shall furthermore ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

For the purpose of the Directive an advanced electronic signature means an electronic signature that meets the following requirements:

- a it is uniquely linked to the signatory
- b it is capable of identifying the signatory
- c it is created using means that the signatory can maintain under his sole control; and
- d it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Any laws, regulations and administrative provisions necessary to comply with this directive should have been brought into force before 19 July 2001. The Directive is therefore applicable in all the Member States today.

6.2.2.3 US

Within the US there is no equivalence to an "advanced electronic signature" as defined by the European Directive.

The use of electronic signatures is regulated by The Electronic Signatures in Global and National Commerce Act (the E-SIGN Act). Under the E-SIGN Act, an "Electronic Signature" is defined as "an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Moreover, contract or other record may not be denied legal effect because it is in an electronic format and a contract may not be denied legal effect solely because an electronic signature was used in its formation.

The E-SIGN Act is technology-neutral and does not require a specific type or method that businesses and consumers must use or accept in order to conduct their electronic transaction. Under the E-SIGN Act, the validity and enforceability of an electronic contract is still evaluated under existing substantive contract law. Therefore, if a statute, regulation or other rule of law requires a contract to be in writing, then an electronic contract must be in a form that is capable of being retained and accurately reproduced at the time of entering into the contract. If an electronic contract meets the validity requirement of a written contract under existing substantive contract law, it is then legally enforceable.

6.2.3 Certification Authority obligations

Any Certification Authority (CA) or Certification Service Provider (CSP), which satisfies the following conditions, may issue certificates provided that:

- 1 The CA undertakes to conform to the stipulations of this Certificate Value Statement; and
- 2 The CA publishes a Certificate Policy defining its legal and financial liability.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

The CA's key management shall be carried out in such a way that recovery of the private key aimed for electronic signatures is never possible. All key management system for generation, provision, validation, real-time validation, recovery or revocation must also have a security level that complies with the provisions set out in the Ericsson Security Policies. Ericsson reserves the right to review the management system and reject any solutions not fulfilling adequate level of security.

Issued certificates shall be published in a Directory service according to current established standards. The Directory service shall be available via the LDAP (Lightweight Directory Access Protocol) interface.

The CA shall continuously generate lists of revoked certificates (certificate revocation lists). The most current list shall be made publicly available in the CA's Directory. Information on revoked certificates shall be stored in the certificate revocation list.

The CA is responsible to revoke a certificate when any of the conditions set out in section 6.2.12. applies.

The CA's private key used for issuing certificates shall only be used for signing certificates and CRLs. The CA is obliged to take the measures necessary to protect its private keys and ensure that these are not used after the validity period for the respective certificates has expired. If unauthorized access to the CA's private keys is suspected, the CA must undertake the following measures:

- 1 Inform all certificate holders about the event.
- 2 Immediately cease the certificate revocation check service relating to the keys to which an unauthorized access is suspected.
- 3 As soon as reasonably practicable revoke the certificates that have been generated using the keys to which an unauthorized access is suspected.

The CA shall undertake to identify the certificate holder requesting revocation by means that support an efficient and reliable revocation service consistent with its policy.

CAs shall, for audit purposes, archive, and make available upon authorized request, documentation of the CA's compliance with its CP and this CVS and documentation of actions and information that is material to each certificate application and to each certificate issued. For each certificate, including the CA-certificates, the records need to extend to the creation, issuance, use, revocation, expiration, and renewal activities. Audits shall be performed at the least annually.

In the event of a corporate decision to terminate the CA, termination shall be done in accordance with procedures specified separately by the CA administration organization. In rough outline, these procedures shall concern e.g.;

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

- How to inform the certificate holders about the termination.
- The continued keeping of certificates in the directory through their validity period.
- The continued keeping of archives according to specified retention time as stated in the CA's CP.

The CA is responsible for drawing up an agreement with the prospective Certificate holder in a way that clearly indicates the rights and obligations of the involved parties.

The CA has to state very clearly that the Certificate holder, by his/her signature, acknowledges the reception of a certificate and the correctness of the information given, and accepts the rules and conditions associated with usage of the certificate.

The CA is responsible for drawing up an agreement with all RAs/LRAs, operating on behalf of the CA, in a way that clearly indicates the rights and obligations of all parties.

All processing of personal data are to be performed in accordance with the provisions set out in the Ericsson Privacy Regulations.

6.2.4 Registration Authority obligations

Any Registration Authority (RA), or Local Registration Authority (LRA) since there may be several RA's depending upon the physical location of the Certificate holders, which satisfies the following conditions may operate within the scope of this Certificate Value Statement:

- 4 the RA shall undertake to conform to the stipulations of this Certificate Value Statement and the Certificate Policy of the CA in question;
- 5 the RA shall register with, and obtain the approval of, a CA that issues certificates in accordance with this Certificate Value Statement.

An RA shall be directly accountable for the transactions it performs on behalf of the CA.

The RA/LRA is responsible for gathering all information required, and for ensuring the correctness of this information, which is required by the CA for the issue of certificates. The RA/LRA shall undertake to continuously update the personal data and other information required for the CA to be able to fulfill its obligations within the CA business activities.

Only applications signed by authorized persons are to be passed by to the CA for the purpose of certificate issuance. Certificates may only be issued in accordance with the rules applicable for authority to sign for an Ericsson Company, as set out in Group Policy "Signing and authorization". This means that two Company signatories jointly are authorized to issue certificates, except in case mandatory provision in local legislation provide otherwise.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

The RA/LRA is responsible for taking delivery of the certificates from the CA and is further responsible for ensuring that the final distribution of certificates to the Certificate holders is carried out in a secure manner. Security measures must comply with the provisions set out in the Ericsson Security Policies. Ericsson reserves the right to review the procedures for handling the delivery of the certificates and reject any solutions not fulfilling adequate level of security.

RA's and LRA's shall carry out their services in accordance with the conditions and obligations required by this CVS, the CA's Certificate Policy and Certificate Practice Statement (CPS), the Ericsson Security and Risk Management Directive, Ericsson Privacy Regulations and any other relevant Ericsson Policies, Directives and Guidelines.

6.2.5 Requesting party obligations

Only authorized persons are allowed to apply for a "Company Liability High"-certificate. The authorized person shall:

- 6 Authenticate itself to CA or RA/LRA according to Ericsson security requirements.
- 7 Present information to be certified and/or to be filed along with the certificate application.
- 8 Sign the certificate application.

The authorized person is responsible for its requests to issue certificates and that the information regarding the certificate holder that has been provided in the request to issue certificates is complete, accurate and properly authorized.

6.2.6 Relying party obligations

It is the responsibility of the Relying party to check the status of the certificate, either by checking the most recently published certificate revocation list or to use the CA's online certificate status service, to ensure that the relevant certificate is currently valid.

The Relying party shall ensure that the certificate is checked against a certificate revocation list that:

- 9 represents the most recent, current revocation information for the certificate in question,
- 10 is valid, i.e. has not expired, and
- 11 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.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

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

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 provided for in the CA's CP or in any other specified terms. It is further the responsibility of the Relying party to ensure that the certificate fulfils the Relying party's requirements as to security and that the certificate is suitable for the purpose in question.

It is the relying party's responsibility to check for certificate revocation prior to accepting the validity of a digital 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.

6.2.7 Certificate holder obligations

By accepting a certificate issued under this CVS, a Certificate holder certifies to and agrees that from the time of certificate acceptance and throughout the operational period of the certificate, until notified otherwise:

- 12 No other individual will be given access to the private key received and accepted by the certificate holder.
- 13 All representations made by the certificate holder to the CA or RA/LRA regarding the information (name, validity period, issuer e t c) in the certificate are true.

The certificate shall be regarded and handled as an item of value. The certificate holder is obliged to retain control of its private key and take precautions to prevent its loss, disclosure to any other party, modification, or unauthorized use.

The Certificate holder is, during the certificate's validity period, responsible for notifying the CA without delay if its keys have been stolen, lost or compromised, if control over private keys has been lost due to loss of activation data (PIN code) or for any other reason, and if inaccuracies or changes in the contents of the certificates is suspected to have occurred.

The Certificate holder is responsible to follow any restrictions given by the CA, RA or LRA on the use of the certificate and to follow any other instructions given regarding the handling of the certificate.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

6.2.8 Certificate Profile

The certificate profiles are to be set in accordance with the recommendation in the IETF RFC 3280. The key usage extension is important and shall have the following value:

- KeyUsage ::= nonRepudiation
- Marked as critical

6.2.9 Requirements for issuing certificates

“Company Liability High”-certificates may only be issued at the request of an authorized person as defined in paragraph 6.2.4.

“Company Liability High”-certificates may be issued to

- 1 Internal certificate holder, which means
 - a. a natural person employed by or reporting to a manager at Ericsson and who is authorized to represent Ericsson, and
 - b. who will create signatures using means that the certificate holder can and will maintain under his/her sole control.

6.2.10 Certificate usage

Company Liability High-certificates may only be used in order to obtain legally binding signatures on a company level and for the purpose of non-repudiation and/or confidentiality.

- “Company Liability High”-certificates must be protected by a hardware mechanism that are to remain under the sole control of the signatory during signing and storage.

The certificates may be used for the following business functions:

Legally binding signatures	Signed electronic information will have legal acceptance, thus binding Ericsson.
Non-repudiation	Ericsson will not be able to deny source of origin.

6.2.11 Ownership rights

The right of ownership and all rights and liabilities regarding certificates and keys issued by any Ericsson company acting as a CA may not be transferred to an entity outside the Ericsson organization.

6.2.12 Revocation

The certificates are to be revoked if one or several of the following events occur:

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

- 14 the information in the certificate is or is suspected to be incorrect,
- 15 unauthorized access or suspected unauthorized access has been gained to the private key,
- 16 the private signature key has been destroyed,
- 17 any agreement regarding the CA-service has ceased to apply,
- 18 a revocation request has been received from the RA, LRA or certificate holder,
- 19 unauthorized access or suspected unauthorized access has been gained to the CA's private key used for issuing certificates, or
- 20 the CA ceases its CA business activities.

6.3 Company Liability Low

6.3.1 Summary

“Company Liability Low”-certificates are aimed to be used in order to obtain electronic records that are not denied legal effect and to meet legal requirements for non-repudiation with regards to originator of an electronic record. Any certificate issued as a “Company Liability Low”-certificate must therefore comply with relevant current legislation.

The “Company Liability Low”-certificates are not aimed at creating legally binding signatures per se, but could be used for signatures supported by contractual means.

In order for Ericsson 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.

6.3.2 Legal and organizational requirements

6.3.2.1 Ericsson

The Ericsson requirements on a “Company Liability Low”-certificates are that the electronic records one may create by using the certificates are not to be denied legal effect within all the regions where Ericsson are represented. Any electronic record secured with such a certificate should meet the legal standards required for non-repudiation with regards to the originator of the record.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

6.3.2.2 EU

When it comes to the legal effect of electronic signatures the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures state that the Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- a in electronic form, or
- b not based upon a qualified certificate, or
- c not based upon a qualified certificate issued by an accredited certification-service-provider, or
- d not created by a secure signature-creation device.

Any laws, regulations and administrative provisions necessary to comply with this directive should have been brought into force before 19 July 2001. The Directive is therefore applicable in all the Member States today.

6.3.2.3 US

The use of electronic signatures is regulated by The Electronic Signatures in Global and National Commerce Act (the E-SIGN Act). Under the E-SIGN Act, an "Electronic Signature" is defined as "an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Moreover, contract or other record may not be denied legal effect because it is in an electronic format and a contract may not be denied legal effect solely because an electronic signature was used in its formation.

The E-SIGN Act is technology-neutral and does not require a specific type or method that businesses and consumers must use or accept in order to conduct their electronic transaction. Under the E-SIGN Act, the validity and enforceability of an electronic contract is still evaluated under existing substantive contract law. Therefore, if a statute, regulation or other rule of law requires a contract to be in writing, then an electronic contract must be in a form that is capable of being retained and accurately reproduced at the time of entering into the contract. If an electronic contract meets the validity requirement of a written contract under existing substantive contract law, it is then legally enforceable.

6.3.3 Certificate Authority obligations

Any Certification Authority (CA) or Certification Service Provider (CSP), which satisfies the following conditions, may issue certificates provided that:

- 21 The CA undertakes to conform to the stipulations of this Certificate Value Statement; and

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

22 The CA publishes a Certificate Policy defining its legal and financial liability.

The CA's key management shall be carried out in such a way that recovery of the private key aimed for electronic signature is never possible. All key management system for generation, provision, validation, real-time validation, recovery or revocation must also have a security level that complies with the provisions set out in the Ericsson Security Policies. Ericsson reserves the right to review the management system and reject any solutions not fulfilling adequate level of security.

Issued certificates shall be published in a Directory service according to current established standards. The Directory service shall be available via the LDAP (Lightweight Directory Access Protocol) interface.

The CA shall continuously generate lists of revoked certificates (certificate revocation lists). The most current list shall be made publicly available in the CA's Directory. Information on revoked certificates shall be stored in the certificate revocation list.

The CA is responsible to revoke a certificate when any of the conditions set out in section 6.3.12. applies.

The CA's private key used for issuing certificates shall only be used for signing certificates and CRLs. The CA is obliged to take the measures necessary to protect its private keys and ensure that these are not used after the validity period for the respective certificates has expired. If unauthorized access to the CA's private keys is suspected, the CA must undertake the following measures:

23 Inform all certificate holders about the event.

24 Immediately cease the certificate revocation check service relating to the keys to which an unauthorized access is suspected.

25 As soon as reasonably practicable revoke the certificates that have been generated using the keys to which an unauthorized access is suspected.

The CA shall undertake to identify the certificate holder requesting revocation by means that support an efficient and reliable revocation service consistent with its policy.

CAs shall, for audit purposes, archive, and make available upon authorized request, documentation of the CA's compliance with its CP and this CVS and documentation of actions and information that is material to each certificate application and to each certificate issued. For each certificate, including the CA-certificates, the records need to extend to the creation, issuance, use, revocation, expiration, and renewal activities. Audits shall be performed at the least annually.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

In the event of a corporate decision to terminate the CA, termination shall be done in accordance with procedures specified separately by the CA administration organization. In rough outline, these procedures shall concern e.g.;

- How to inform the certificate holders about the termination.
- The continued keeping of certificates in the directory through their validity period.
- The continued keeping of archives according to specified retention time as stated in the CA's CP.

The CA is responsible for drawing up an agreement with the prospective Certificate holder in a way that clearly indicates the rights and obligations of the involved parties.

The CA has to state very clearly that the Certificate holder, by his/her signature, acknowledges the reception of a certificate and the correctness of the information given, and accepts the rules and conditions associated with usage of the certificate.

The CA is responsible for drawing up an agreement with all RAs/LRAs, operating on behalf of the CA, in a way that clearly indicates the rights and obligations of all parties.

All processing of personal data are to be performed in accordance with the provisions set out in the Ericsson Privacy Regulations.

6.3.4 Registration Authority obligations

Any Registration Authority (RA), or Local Registration Authority (LRA) since there may be several RA's depending upon the physical location of the Certificate holders, which satisfies the following conditions may operate within the scope of this Certificate Value Statement:

- 26 the RA shall undertake to conform to the stipulations of this Certificate Value Statement and the Certificate Policy of the CA in question;
- 27 the RA shall register with, and obtain the approval of, a CA that issues certificates in accordance with this Certificate Value Statement.

An RA shall be directly accountable for the transactions it performs on behalf of the CA.

The RA/LRA is responsible for gathering all information required, and for ensuring the correctness of this information, which is required by the CA for the issue of certificates. The RA/LRA shall undertake to continuously update the personal data and other information required for the CA to be able to fulfill its obligations within the CA business activities.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

Only applications signed by authorized persons are to be passed by to the CA for the purpose of certificate issuance.

Authorized persons are:

- President
- CFO

The RA/LRA is responsible for taking delivery of the certificates from the CA and is further responsible for ensuring that the final distribution of certificates to the Certificate holders is carried out in a secure manner. Security measures must comply with the provisions set out in the Ericsson Security Policies. Ericsson reserves the right to review the procedures for handling the delivery of the certificates and reject any solutions not fulfilling adequate level of security.

RA's and LRA's shall carry out their services in accordance with the conditions and obligations required by this CVS, the CA's Certificate Policy and Certificate Practice Statement (CPS), the Ericsson Security Policies, the Ericsson Privacy Regulations and any other relevant Ericsson Policies, Directives and Standards.

6.3.5 Requesting party obligations

Only authorized persons are allowed to apply for a "Company Liability Low"-certificate. The authorized person shall:

- 28 Authenticate itself to CA or RA/LRA according to Ericsson security requirements
- 29 Present information to be certified and/or to be filed along with the certificate application.
- 30 Present details regarding the Electronic internal certificate holder to be certified and/or to be filed along with the certificate application. Information such as type of system, system name/ID, other technical details, number of certificate holders, and geographical location of server.
- 31 Sign the certificate application.

The authorized person is responsible for its requests to issue certificates and that the information regarding the certificate holder that has been provided in the request to issue certificates is complete, accurate and properly authorized.

If the certificate holder is not a person, but a system, the authorized person must create and store a valid instruction, delegating the right to create signatures in the name of the authorized person.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

6.3.6 Relying party obligations

It is the responsibility of the Relying party to check the status of the certificate, either by checking the most recently published certificate revocation list or to use the CA's online certificate status service, to ensure that the relevant certificate is currently valid.

The Relying party shall ensure that the certificate is checked against a certificate revocation list that:

32 represents the most recent, current revocation information for the certificate in question,

33 is valid, i.e. has not expired, and

34 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.

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 provided for in the CA's CP or in any other specified terms. It is further the responsibility of the Relying party to ensure that the certificate fulfils the Relying party's requirements as to security and that the certificate is suitable for the purpose in question.

It is the relying party's responsibility to check for certificate revocation prior to accepting the validity of a digital 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.

6.3.7 Certificate holder obligations

By accepting a certificate issued under this certificate policy, a Certificate holder certifies to and agrees that from the time of certificate acceptance and throughout the operational period of the certificate, until notified otherwise:

35 No other individual will be given access to the private key received and accepted by the certificate holder.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

36 All representations made by the certificate holder to the CA or RA/LRA regarding the information (name, validity period, issuer e t c) in the certificate are true.

If the certificate holder is not a person, but a system, the authorized person must create and store a valid instruction, delegating the right to create signatures in the name of the authorized person.

The certificate shall be regarded and handled as an item of value. The certificate holder is obliged to retain control of its private key and take precautions to prevent its loss, disclosure to any other party, modification, or unauthorized use.

The Certificate holder is, during the certificate's validity period, responsible for notifying the CA without delay if its keys have been stolen, lost or compromised, if control over private keys has been lost due to loss of activation data (PIN code) or for any other reason, and if inaccuracies or changes in the contents of the certificates is suspected to have occurred.

The Certificate holder is responsible to follow any restrictions given by the CA, RA or LRA on the use of the certificate and to follow any other instructions given regarding the handling of the certificate.

6.3.8 Certificate Profile

The certificate profiles are to be set in accordance with the recommendation in the IETF RFC 3280. The key usage extension is important and shall have the following value:

- KeyUsage ::= digitalSignature
- Marked as critical

6.3.9 Requirements for issuing certificates

“Company Liability Low”-certificates may only be issued at the request of an authorized person as defined in paragraph 6.3.4.

“Company Liability Low”-certificates may be issued to the following:

- 37 Internal Certificate Holder, which means a natural person employed by or reporting to a manager at Ericsson and who is authorized to represent Ericsson.
- 38 Electronic Internal Certificate Holder, which means the system owner of a program, process, etc. which automatically creates electronic signatures and which is owned or controlled by Ericsson.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

6.3.10 Certificate usage

Company Liability Low-certificates may only be used in order to create electronic records with legal effect and for the purpose of non-repudiation and/or confidentiality.

The certificates may be used for the following business functions:

Electronic records	Signed electronic information cannot be refused as electronic records with legal effect.
Non-repudiation	Ericsson will not be able to deny source of origin.

6.3.11 Ownership rights

The right of ownership and all rights and liabilities regarding certificates and keys issued by any Ericsson company acting as a CA may not be transferred to an entity outside the Ericsson organization.

6.3.12 Revocation

The certificates are to be revoked if one or several of the following events occur:

- 39 the information in the certificate is or is suspected to be incorrect,
- 40 unauthorized access or suspected unauthorized access has been gained to the private key,
- 41 the private signature key has been destroyed,
- 42 any agreement regarding the CA-service has ceased to apply,
- 43 a revocation request has been received from the RA, LRA or certificate holder,
- 44 unauthorized access or suspected unauthorized access has been gained to the CA's private key used for issuing certificates, or
- 45 the CA ceases its CA business activities.

6.4 Non-Liability

Any type of certificate issued by, or on behalf of, an Ericsson Entity that does not comply with the regulations in this Certificate Value Statement.

When issuing Non-Liability certificates Ericsson shall disclaim all express or implied conditions, representations and warranties, including any implied warranty of merchantability, satisfactory quality, fitness for a particular purpose or non-infringement, except to the extent that such disclaimers are held to be legally invalid.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

Ericsson shall further, to the maximum extent permissible by applicable law, accept no liability for any direct, punitive, special, incidental and consequential damages arising out of or relating to the use of Non-Liability certificates (including loss of business, revenue, profits, use, data or other economic advantage) however it arises, whether for breach or in tort.

7 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.

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

8 Definitions

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.
Certificate	An electronic certificate, stamped by the issuer, confirming that a public key belongs to a certain entity.
Certificate holder	A holder (entity) of a certificate approved 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 that a certificate has not been revoked.
Certificate revocation list	Lists maintained by the CA containing the identities of all certificates that have been revoked.
Certificate Value Statement	Rules establishing the minimum requirements for the issuing and use of electronic signatures within Ericsson. The CVS, together with the company's CP, thus describes the requirements that the certification body has undertaken to fulfil.
Certification Authority (CA)	An entity that is responsible for issuing and signing certificates.
Directory	An electronic register that contains certificates, public keys and certificate revocation lists.
Directory service	Provision of access to the Directory named above.
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 entity who appears to be issuer, and that the content 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.
Key generation	The process that creates both public and private keys.
Local Registration Authority	A local registration body of the CA. An entity that is responsible for identification and authentication of

Prepared (also subject responsible if other) LME/D/AB Bo Eklund		No. LME/DA-04:000096 Uen		
Approved LME/D/A [Hans Dahlquist]	Checked LMEMODE	Date 2004-11-23	Rev A	Reference

(LRA)	certificate subjects, but that does not sign or issue certificates.
Private keys	The secret part of a pair of keys that is used for decryption or signature.
Public keys	The public part of a pair of keys that is used for encryption or verification.
Registration Authority	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.
Relying party	Entity which receives data that has been signed and/or encrypted by a certificate issued by the CA.
Revocation	A marking that a certificate should no longer be considered reliable.
Signature verification data	Data used to verify an electronic signature.