Roccade Megaplex B.V.

Certificate Practice Statement

Version 1.0

CPS Steering Committee

10 June 1999

List of abbreviations

CA	Certification Authority
CK	Common Key
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DAM	Draft amendment (to an ISO standard)
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IA	Issuing Authority
LRA	Local Registration Authority
LRAA	Local Registration Authority Administrator
NSI	Nonverified Subscriber Information
PCA	Primary Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RDN	Relative Distinguished Name
RSA	a cryptographic system (*see* definitions)
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
VDPE	VeriSign Distinguished Panel of Experts
MR	MegaSign Root
MSP	MegaSign Security Procedures
WWW or Web	World Wide Web
X.509	the ITU-T standard for certificates and their corresponding authentication framework

1 Introduction

1.1 Overview

a) Summary

This MegaSign Certification Practice Statement (CPS), as well as the associated Certificate Policies (CPs), presents the practices that MegaSign (which is part of Roccade Megaplex), its Issuing authorities (IAs), and authorized non-MegaSign employ in issuing and managing certificates and in maintaining a certificate-based Public Key Infrastructure (PKI) It details and controls the certification process, from establishing IAs, commencing IA and repository operations, to enrolling subscribers. The MegaSign Certification Services (MCS) provides for issuing, managing, using, suspending, revoking, and renewing of certificates.

The CPS, as well as the associated CPs, is intended to legally bind and provide notice to all parties that create, use, and validate certificates within the context of the MCS. As such, the CPS plays a central role in governing the MCS.

This CPS governs only a portion of the complement of services offered by MegaSign. Other MegaSign services may neither require nor invoke a hierarchy of IAs. The MCS will inevitably evolve to accommodate other structures in response to market demand. This CPS, as well as the associated CP's, is periodically updated to reflect new services and to improve the MCS infrastructure in general (See CPS § 8.1.).

b) Structure of the CPS and CPs

The MegaSign CPS is a statement of the practices which any MegaSign IA employs in issuing certificates. The framework used for describing the whole set of practices is compliant with the PKIX-4 standard of the IETF. Currently there are three different classes of certificates representing different levels of trustworthiness described in a specific CP. The certificate classes also refer to the different application of the certificate. For MegaSign CPs see the MegaSign repository (http://www.megasign.nl/repository).

Each class of certificate is characterized by a different level of the following properties:

- confirmation of identity (such as through personal presence or investigation),
- IA private key protection (and assurance of appropriate use),
- certificate applicant and subscriber private key protection, and operational controls.

While the certificates (and MegaSign's supporting products and services) possess many other properties, those certificates provide a framework for distinguishing some of their aspects that affect their relative trust.

c) Customer service assistance, education, and training

This CPS assumes that the reader is generally familiar with digital signatures, PKIs, and MCS. If not, we advise some training in the use of public key techniques before the reader applies for a certificate. Educational and training information is accessible from MegaSign at http://www.megasign.nl/repository.

ALL MCS APPLICANTS AND SUBSCRIBERS ACKNOWLEDGE THAT (i) THEY HAVE BEEN ADVISED TO RECEIVE PROPER TRAINING IN THE USE OF PUBLIC KEY TECHNIQUES PRIOR TO APPLYING FOR A CERTIFICATE AND THAT (ii) DOCUMENTATION, TRAINING, AND EDUCATION ABOUT DIGITAL SIGNATURES, CERTIFICATES, PKI, AND THE MCS ARE AVAILABLE FROM MEGASIGN.

d) Additional services

Certificates generated by VeriSign in the USA, will have an extended warranty protection under the NetSure^{SM} Protection Plan to subscribers obtaining certificates on or after its effective date. The NetSure^{SM} Protection Plan is available in the VeriSign repository at **https://www.verisign.com/repository/netsure**. For further information, see the FAQ regarding the NetSure^{SM} Protection Plan at **https://www.verisign.com/repository/netsure_faq.**

In the near future MegaSign will provide a comparable protection plan for certificates generated in The Netherlands.

e) Test certificates

Test certificates may be issued for authorized testing purposes only. Test certificates are issued from the MegaSign/VeriSign Test CA, which is independent of the MegaSign and VeriSign CPS. It is controlled by the specific CPS. See applicable repository for details. Only authorized persons may use test certificates. Note: The information contained within a test certificate shall be considered non-verified subscriber information (NSI).

1.1.1 Certificate Classes

1.1.1.1 Class 2 certificates

Class 2 certificates are currently issued to individuals only. Class 2 certificates confirm that the application information provided by the subscriber does not conflict with information in well-recognized consumer databases. In addition, using VeriSign OnSite, MegaSign's enterprise customers may take on the role of a non-MegaSign organizational local registration authority (LRA) in order to approve (or disapprove) the issuance of Class 2 certificates to its own employees and other affiliated individuals (for individual certificates) or organizations (for server certificates). Validation is based on checking appropriate internal documentation (such as human resources (HR) employee and independent contractor rolls).

1.1.1.2 Class 3 certificates

Class 3 Certificates are issued to individuals and organizations.

1.1.1.2.1 Class 3 individual certificates

Class 3 certificates provide important assurances of the identity of individual subscribers by requiring their personal (physical) appearance before a Class 3 LRA or its delegate. Another type of Class 3 individual certificate is the "Class 3 LRAA certificate." It is issued for authorized LRAA purposes only, exclusively to certain approved LRA Administrators (LRAAs) employed by non-MegaSign organizational LRAs. The LRAA must be authorized by the applicable LRA (via authenticated record) as a prerequisite to LRAA certificate approval.

1.1.1.2.2 Class 3 organizational certificates

Class 3 certificates can provide assurances of the existence and name of various public- and private-sector organizations (such as government agencies and corporations).

1.2 Identification

Certification Practice Statement Name:

Roccade MegaSign Certification Practice Statement version 1.0

Object Identifier:

Roccade MegaSign CPS: 0.3.2062.9.Roccade MegaSign (6).CPS(0).Version(1)

1.3 Community and applicability

The MegaSign CPS has been designed to provide a statement of the practices that IAs within the MegaSign infrastructure employ in issuing certificates. The applicability of the certificates issued by IAs in accordance with this CPS will be documented in the associated CPs.

1.3.1 Certification authorities

In accordance with the provisions of the MegaSign CPS, the following IAs can be distinguished within the MegaSign Certification Services (MCS).

1.3.2 Registration authorities

In accordance with the provisions of this CPS, the following Registration Authorities (RA) can be distinguished within the MegaSign infrastructure:

- MegaSign
- MegaSign authorized (L)RA's.
- MegaSign customers using Onsite service (LRA's)

Local registration authorities (LRAs) are entities that evaluate and approve or reject certificate applications. LRAs also have the authority to approve the revocation (or where authorized, suspension) of certificates. LRAs may employ LRA Administrators LRAAs) to perform the work of the LRA. LRAs operate on behalf of and (within the context of the CPS) under the exclusive authority of a single IA (the VR, PCA or CA that actually issues the certificates). An IA may have more than one LRA.

Non-MegaSign organizational LRAs are MegaSign OnSite customer LRAs not affiliated with MegaSign that are authorized to approve the issuance and revocation of certificates to affiliated individuals within the LRA's organization. For example, a company may become a non-MegaSign organizational LRA in order to approve (or disapprove) the issuance of certificates to its own employees and other affiliated individuals and may not approve the issuance of certificates to the general public.

Certificates issued by non-MegaSign organizational LRAs may only be issued to individuals whose affiliation with the LRA is ascertainable by the LRAA via appropriate internal documentation (such as human resources (HR) employee and independent contractor rolls). All certificates issued as a result of a non-MegaSign organizational LRA's approval of a certificate application shall contain a distinguished name that states the affiliation of its subject. Non-MegaSign organizational LRAs are exclusively responsible for approving or not approving certificate applications. Consequently, VeriSign, MegaSign, and IAs disclaim all such responsibility.

1.3.3 End entities

In accordance with the corresponding CP, subscribers that are the subject of the issued certificates may be:

- any natural person which can be uniquely identified by a valid proof of identity. Please see applicable CP for details.
- any legal person which can be uniquely identified.
- any other object (e.g. server) that can be uniquely identified.

1.3.4 Applicability

a) Suitable applications

An overview of certificate applications is shown in the table below. See the applicable CP for details.

	Summary of Confirmation of Identity	IA Private Key Protection	Certificate Applicant and Subscriber Private Key Protection	Applications implemented or contemplated by Users -See CPS § 1.1.1(a) Disclaimer & § 5.
Class 2	Automated unambiguous name and E-mail address search, plus automated enrollment information check plus automated address check	PCA & CA: trustworthy hardware	Encryption software (PIN protected) required	Individual and intra- and inter-company E-mail, on-line subscriptions, password replacement, and software validation
Class 3	Automated unambiguous name and E-mail address search, plus personal presence & ID documents plus Class 2 automated ID check for individuals; business records (or filings) for organizations	PCA & CA: trustworthy hardware	Encryption software (PIN protected) required; hardware token recommended but not required	E-banking, corp. database access, personal banking, membership-based on-line services, content integrity services, E-commerce server, software validation; authentication of LRAAs; and strong encryption for certain servers

b) Approved applications

Only the applications suitable for a particular certificate will be approved. See the above table and applicable CP.

c) Prohibited applications

It is prohibited to use certificates issued in accordance with this CPS for another purpose than as defined for that certificate type in the list of suitable applications. The set of rules set forth in the applicable CP also applies.

Contact Details

1.4.1 Specification administration organization

This CPS is administered by MegaSign. CPS administration is done in accordance with chapter 8 of this CPS.

1.4.2 Contact person

All requests and comments concerning this CPS can be addressed to:

Roccade Megaplex BV
attn: MegaSign CPS Board
PO Box 9105
7300 HN APELDOORN

http://www.MegaSign.nl
E-mail: digitalidcentre@megaplex.nl
Tel: +31(0)55 577 8432
Fax: +31(0)55 577 8810

MegaSign is a service of
Roccade Megaplex B.V.

1.4.3 Person determining CPS suitability for the policy

a) The MegaSign CPS Board is responsible for determining the customer policy suitability for the MegaSign/VTN CPS and this has to be approved by the association of Worldwide VeriSign-affiliates (VTN Members). An independent IT-auditor will audit this approval worldwide for each VTN member.

b) The MegaSign CPS Board is responsible for determining and issuing the CPS. The CPS Board is also responsible for determining different CPs and their suitability to CPS. The CPS board is responsible for authorizing CAs to issue certificates under a particular MegaSign CP.

c) The MegaSign CPS Board is responsible for initiating audits as stated in section 2.7.1.

d) To contact the MegaSign CPS Board, please use the contact information as stated in section 1.4.2.

2 General provisions

2.1 Obligations

This CPS section defines the obligations of the IA, RA, LRA, subscriber, relying party and repository. Additional obligations may be defined in the applicable CPs and in ancillary agreements.

2.1.1 IA obligations

The following are the obligations of any IA within the MegaSign infrastructure:

a) Compliance with CPS, CPs and ancillary agreements

The IA is obliged to comply with all provisions in this CPS, in applicable CPs and in applicable ancillary agreements in performing its services [hereinafter defined as 'applicable provisions']. IAs shall utilize only trustworthy systems in performing their respective services. For purposes of this CPS, "**TRUSTWORTHY SYSTEM**" means computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

b) Notification of certificate issuance - to subscriber

The IA is obliged to notify the subscriber who is the subject of the certificate upon issuance of the certificate.

c) Notification of certificate issuance - to others

The IA is obliged to notify other parties than the subscriber of the certificate issuance by publishing the certificate in the MegaSign repository.

d) Notification of certificate revocation - to subscriber

The IA is obliged to notify the subscriber who is the subject of the certificate of the certificate revocation. Section 4.4 of this CPS is likewise applicable.

e) Notification of certificate revocation - to others

If a certificate is revoked the IA is obliged to notify other parties by publishing the certificate in the CRL. Section 4.4 of this CPS is likewise applicable.

f) IAs private key protection

Any IA within the MegaSign infrastructure is obliged to protect its private key as well as the activation data providing access to this key. Section 6.2 of this CPS is likewise applicable.

g) Restriction on IAs private key use

Any IA within the MegaSign infrastructure is obliged to use its private key only for issuing certificates and CRLs in accordance with the applicable provisions.

h) Privacy

Non-MegaSign IA

Any non-MegaSign IA is obliged to collect and process personal data in accordance with applicable data protection legislation and regulations. The non-MegaSign IA is responsible for the processing of the

personal data of the subscribers.

MegaSign IA
Roccade Megaplex B.V. is responsible ('houder' within the meaning of the Wet persoonsregistraties and 'verantwoordelijke' within the meaning of the Wet bescherming persoonsgegevens) for the processing by MegaSign IAs of the personal data of the subscribers as defined in section 1.3.1 of this CPS. MegaSign IAs process the personal data of these subscribers in accordance with the Wet persoonsregistraties and, in the future, in accordance with the Wet bescherming persoonsgegevens. The Dutch Data Protection Authority (Registratiekamer) has been notified regarding the collection of personal data by MegaSign. The goal for which the personal data of the subscribers are collected is stated in this notification. Subscribers can contact Roccade Megaplex B.V. at the address specified in section 1.4.2 in order to gain access to his/her personal data and make use of his/her right to correct data.

i) Misrepresentation in certificate

The information that was submitted by subscriber/applicant during certificate application is considered to be error free. If subscriber can provide evidence that misrepresentations of certificate content are imputable to the IA that issued the certificate, the IA is obliged to correct this within ***one working day*** by providing a new certificate.

j) Any further liability concerning misrepresentations of certificate content is explicitly excluded.

2.1.2 RA obligations

The following are the obligations of any RA within the MegaSign infrastructure. These obligations also apply to any IA within the MegaSign infrastructure which is also a RA.

a) Compliance with CPS, CPs and ancillary agreements

The RA is obliged to comply with the applicable provisions in performing its services. RAs shall utilize only trustworthy systems in performing their respective services.

b) Application validation and accuracy of representations

The RA is obliged to perform the necessary application validation procedures and accurately represent the application information that is provided by the applicant/subscriber during the application procedure to the IA, in accordance with applicable provisions.

c) Maintain certificate application information

The RA is obliged to keep supporting evidence for any certificate request made to an IA (e.g., certificate request forms) in accordance with applicable provisions. The information provided by the applicant/subscriber in the certificate request that is not included in the certificate will be kept confidential by the RA.

d) Privacy

Delegated MegaSign RAs
RAs within the MegaSign infrastructure are obliged to collect and processes personal data in accordance with applicable data protection legislation and regulations. The delegated MegaSign RA is responsible for the processing of the personal data of the subscribers.

MegaSign RA
Roccade Megaplex B.V. is responsible ('houder' within the meaning of the Wet persoonsregistraties and 'verantwoordelijke' within the meaning of the Wet bescherming persoonsgegevens) for the processing by MegaSign RAs of the personal data of the subscribers as defined in section 1.3.1 of this CPS. MegaSign RAs process the personal data of these subscribers in accordance with the Wet

persoonsregistraties and, in the future, in accordance with the Wet bescherming persoonsgegevens. The Dutch Data Protection Authority (Registratiekamer) has been notified regarding the collection of personal data by MegaSign. The goal for which the personal data of the subscribers are collected is stated in this notification. Subscribers can contact Roccade Megaplex B.V. at the address specified in section 1.4.2 in order to gain access to his/her personal data and make use of his/her right to correct data.

e) RAs private key protection

Any RA within the MegaSign infrastructure is obliged to protect its private key as well as the activation data providing access to this key. Section 6.2 of this CPS is likewise applicable.

f) Notification of IA upon private key compromise

RAs are obliged to notify the IA that issued the certificate upon compromise of their private key or the activation data providing access to this key. The notification is done by submitting a revocation request in accordance with section 4.4 immediately after discovery of the compromise.

Upon compromise of any private key within the MegaSign infrastructure - or the activation data providing access to this key - RAs are obliged to notify the IA that issued the certificate.

g) Restriction on RA private key use

Any RA within the MegaSign infrastructure is obliged not to use its private key than for signing and/or decrypting data in accordance with the applicable provisions.

2.1.3 Subscriber obligations

The following are the obligations of any subscriber within the MegaSign infrastructure:

a) Accuracy of representations in certificate applications

Subscribers shall provide accurate information in their certificate applications and in other communications with the LRA, RA and IA, in accordance with the applicable provisions.

b) Subscriber's private key protection

Subscriber is exclusively responsible for protecting his, her or its private key against compromise. Therefor the subscriber is obliged to protect the private key as well as the activation data providing access to this key at all times against loss, theft, disclosure to any other party, modification, unauthorized use, or any other compromise, in accordance with applicable provisions.

Subscriber guarantees that the private key that corresponds with the public key in the certificate has not been compromised during the period from key-pair generation until certificate application.

Private key compromise as described in the two above-mentioned paragraphs give immediate cause for a notification of IA upon private key compromise as described in the first paragraph of section 2.1.3 sub c.

c) Notification of IA upon private key compromise

Subscribers are obliged to notify the IA that issued the certificate upon compromise of their private key or the activation data providing access to this key. The notification is done by submitting a revocation request in accordance with section 4.4 immediately after discovery of the compromise.

Upon compromise of any private key within the MegaSign infrastructure - or the activation data providing access to this key - subscribers are obliged to notify the IA that issued the certificate.

d) Notification of IA upon any change of certificate content

The subscribers are obliged to notify the IA that issued their certificates upon any change in the content of their certificates by sending the IA a certificate revocation request immediately after change of the certificate content, in accordance with section 4.4 of this CPS. for notifying the IA that issued the certificate upon compromise of the private key or the activation data providing access to this key.

e) Quality of the VTN/MegaSign Certification Services

Subscribers shall not undertake any action that can negatively effect the quality of the technical implementation of the VTN/MegaSign Certification Services, including but not limited to the reliability and the integrity of these Certification Services.

f) Restrictions on private key and certificate use

Subscribers may only use the private key for purposes that correspond with the specific certificate-usage as defined for the different classes of certificates in section 1.3.4 of this CPS and the applicable CP.

g) Indemnification by subscribers

Subscribers shall indemnify MegaSign against all claims by third parties, by whatever name such claims may be known, caused by utilization of certificates inconsistent with section 1.3.4 of this CPS and/or the applicable CP.

h) Verification correctness certificate information

Subscribers are obliged to verify whether the information in the issued certificate corresponds with the information that was submitted by the applicant/subscriber during certificate application.

By using the certificate the subscriber acknowledges that the information in the certificate of the subscriber is correct and complete.

In case the issued certificate contains misrepresentations the subscriber is obliged to immediately inform the IA that issued the certificate by submitting a certificate revocation request, in accordance with section 4.4 of this CPS.

i) Uniqueness public key

The applicant/subscriber guarantees that the public key is not, and will never be, submitted in a certificate request more than once.

j) Notification of IA upon private key compromise

Subscribers are responsible for notifying the IA that issued the certificate upon compromise of the private key or the activation data providing access to this key.

k) Damaging material

Applicants/subscribers will not submit to any IA within the MegaSign infrastructure or the MegaSign repository or any other IA's repository any materials that contain statements that (i) are abusive, slanderous, libelous, defamatory, blasphemous, seditious, indecent, obscene, pornographic, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activity with the intent to commit them, or (iii) otherwise violate Dutch law.

l) Intellectual or industrial property rights and confidentiality notices

Subscribers shall not remove from or change in the software, equipment or materials of any party within

the MegaSign Certification Services any designation concerning copyrights, trademarks, tradenames or other intellectual or industrial property rights, including any indications concerning the confidential nature and secrecy of the software.

m) Certificate applicants (and, upon acceptance, subscribers) represent and warrant that their submission (to an IA) and use of a domain and distinguished name (and all other certificate application information) does not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Certificate applicants (and, upon acceptance, subscribers) shall defend, indemnify, and hold their IA harmless for any loss or damage resulting from any such interference or infringement.

2.1.4 Relying party responsibilities

The following are relying party responsibilities within the MegaSign infrastructure:

a) Take notice of CPS and applicable CP

It is the responsibility of a relying party to take notice of the content of this CPS as well as the applicable CP before relying on the content of a certificate within the MegaSign infrastructure as well as before consulting **Certificate Status Information** to gain information about the status of a certificate within the MegaSign infrastructure.

Relying parties are deemed to have taken notice of the content of this CPS as well as the applicable CP if they rely on the content of a certificate within the MegaSign infrastructure or consult **Certificate Status Information [information in the CRL or any other means of revocation information]** to gain information about the status of a certificate within the MegaSign infrastructure.

b) Use of certificates for suitable purposes

Prior to the use of the certificate, relying parties are responsible to independently assess and determine the suitability of a certificate for a specific purpose in a specific situation, in accordance with this CPS and the associated CP (see: section 1.3.4).

The use of the certificate will deem the acceptance of the certificate by the relying party for a specific purpose and will impose the responsibilities on the relying party as stated in the applicable provisions, irrespective of the fact whether certificate suitability was assessed and determined.

c) Checking the MegaSign (or other IA) repository for revocation or suspension

Prior to its use, relying parties must establish a certificate chain for the certificates on which they wish to rely. Once they establish a certificate chain, they must check each certificate in the certificate for its validity. The relying party must determine if any of the certificates along the chain from the signer to an acceptable root within the MegaSign infrastructure has been revoked or suspended.

d) Digital signature verification responsibilities

Relying parties are responsible for verifying the digital signature of a received digitally signed message and for verifying the digital signatures on all the certificates in the certificate chain.

A relying party who is found to have acted in a manner inconsistent with these responsibilities assumes all risks with regard to it and is not entitled to any presumption that the digital signature is effective as the signature of the subscriber.

e) Notification of IA upon private key compromise

Relying parties are responsible for notifying the IA that issued the certificate upon compromise of the private key or the activation data providing access to this key.

f) Damaging material

Relying parties will not submit to any IA within the MegaSign infrastructure or the MegaSign repository or any other IA's repository materials that contain statements that (i) are abusive, slanderous, libelous, defamatory, blasphemous, seditious, indecent, obscene, pornographic, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activity with the intent to commit them, or (iii) otherwise violate Dutch law.

g) Intellectual or industrial property rights notices

Relying parties shall not remove from or change in the software, equipment or materials of any party within the MegaSign Certification Services any designation concerning copyrights, trademarks, tradenames or other intellectual or industrial property rights, including any indications concerning the confidential nature and secrecy of the software.

2.1.5 Repository obligations

MegaSign will make use of the MegaSign repository to publish issued certificates, CRLs, the CPS, the CPs, ancillary agreements and other relevant information. The MegaSign repository shall conform to this CPS in performing its services. In addition, it shall utilize only trustworthy systems in performing its services.

a) Timely publication of suspension and revocation information

The MegaSign repository is obliged to timely publish the CRL, in accordance with section 4.4 of this CPS.

b) Timely publication of amendments to the CPS and the CPs

The MegaSign repository is obliged to act promptly to publish amendments to the CPS and the CPs for the provision of MegaSign's Certification Services, in accordance with Section 8 of this CPS.

c) Timely publication of certificates

The MegaSign repository is obliged to make certificates available after acceptation by the subscriber of the certificate. Section 4.3 of this CPS applies to certificate acceptance.

d) Timely removal of certificates

The MegaSign repository is obliged to remove certificates from the repository after the certificate validity period, consistent with this CPS.

e) Accessibility of MegaSign repository

The MegaSign repository is accessible at www.megasign.nl/repository and by other communication methods.

2.2 Liability

2.2.1 IA liability

The guarantee obligations of MegaSign and other IAs within the MegaSign infrastructure are limited to what is described in this section, unless different or additional guarantees have been expressly agreed in writing.

MegaSign and other IAs within the MegaSign Infrastructure guarantee to perform their services with care and to the best of their ability, in accordance with the provisions laid down in the CPS, the CPs and ancillary agreements.

The guarantee and the liability of any IA within the MegaSign infrastructure with regard to goods and services supplied by third parties, including, but not limited to, suppliers of the IA and telecom operators, will never exceed the guarantee offered by the third party concerned and the liability in that respect

In no case shall MegaSign or any other IA within the MegaSign infrastructure be deemed to have undertaken to provide a different or a more far-reaching performance than stated in the CPS, the applicable CP and the applicable ancillary agreement. Any recommendations or opinions orally expressed by MegaSign or any other IA within the MegaSign shall not entail any extensions to its obligations.

The guarantee obligations of MegaSign and other IAs within the MegaSign Infrastructure laid down in this section shall cease to apply if any party (including without limitation a subscriber, an applicant, a recipient, or a relying party) has made alterations or caused alterations to be made to what has been delivered by MegaSign or any other IA within the MegaSign Infrastructure without prior written consent of that IA. Moreover MegaSign or any other IA within the MegaSign Infrastructure shall not be obliged to perform guarantee obligations if the defect is the result of conduct (including without limitation negligence and lack of reasonable care) of the above mentioned parties.

Any IA within the MegaSign Infrastructure guarantees, contrary to what has been stated above and possible other guarantee agreements, with regard to the millennium problem that:

a) The IA will exercise reasonable care in the selection of products and/or services of third parties that are essential for the completion of the services of the IA. The IA expressly declines all liability for deficiencies that may occur in the execution of services due to the millennium problem and/or Chain problems caused by the products supplied by third parties and/or the combination of these products and services with the products compiled by the MegaSign Infrastructure on behalf of the customer.

b) The IA will perform the services as set forth in this CPS, the CPs and/or ancillary agreements in the exercise of reasonable care.

However, with regard to the millennium problem, MegaSign or any other IA within the MegaSign Infrastructure expressly refuses all responsibility for failures to meet service levels. Any other guarantee and/or liability of MegaSign or any other IA within the MegaSign Infrastructure concerning the millennium problem is expressly excluded.

Millennium problems

The problems caused by the use of date fields in databases, programs and/or hardware and/or the practice of improperly using certain dates in (information) systems to denote for example unknown or infinite data, which may, around the turn of the century, cause the (information) system to be unable to process these dates without causing deficiencies in the (information) systems and/or the data processed by these programs.

Chain problems:

The problems that may arise when data to be processed by an (information) system, are supplied by a (part of) an (information) system that is not included in an agreement between an IA and another party within the MegaSign Infrastructure and/or are supplied to an (other) (part of an) (information) system that is not included in the agreement.

2.2.1.1 Issuing authority representations to subscribers and relying parties

This section lists the specific representations issuing authorities make upon issuing certificates.

2.2.1.1.1 IA's Representations upon certificate issuance

2.2.1.1.1.1 IA's representations to subscribers

(i) Unless otherwise provided in this CPS or mutually agreed upon by both the IA and the subscriber in an authenticated record, the IA promises to the subscriber named in the certificate that

(a) there are no misrepresentations of fact in the certificate known to the IA or originating from the IA,

(b) there are no data transcription errors as received by the IA from the certificate applicant resulting from a failure of the IA to exercise reasonable care in creating the certificate, and

(c) the certificate meets all material requirements of this CPS.

(ii) Unless otherwise provided in this CPS or mutually agreed upon by both the IA and the subscriber in an authenticated record, the IA promises to the subscriber to make reasonable efforts, consistent with the terms of this CPS,

(a) to promptly revoke or suspend certificates in accordance with CPS §§ 4.4, and

(b) to notify subscribers of any facts known to it that materially affect the validity and reliability of the certificate it issued to such subscriber.

(iii) The obligations and representations in CPS §§ 2.2.1.1.1.1(i) and (ii) are made and undertaken solely for the benefit of the subscriber and are not intended to benefit or be enforceable by any other party. An IA makes reasonable efforts, for purposes of CPS § 2.2.1.1.1.1(ii), if its conduct substantially complies with this CPS and applicable law.

2.2.1.1.1.2 IA's representations to relying parties

By issuing a certificate an IA represents to all who reasonably rely on a digital signature verifiable by the public key listed in the certificate that consistent with this CPS:

(i) all information in or incorporated by reference within the certificate, except nonverified subscriber information (NSI), is accurate, and

(ii) the IA has substantially complied with the CPS when issuing the certificate.

2.2.1.1.2 IA's Representations upon publication

By publishing a certificate (*see* CPS § 2.1.1(c)), an IA certifies to the MegaSign repository and to all who reasonably rely on the information contained in the certificate that it has issued the certificate to the subscriber and that the subscriber has accepted the certificate, as described in CPS § 4.3.

2.2.1.2 Disclaimers of warranties and liability

EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING (CPS §§ 2.2.1.1), ISSUING AUTHORITIES, MEGASIGN, AND VERISIGN DISCLAIM ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE AND LACK OF REASONABLE CARE.

Except as expressly stated in the foregoing CPS §§ 2.2.1.1, IAs, MegaSign, and VeriSign

• do not warrant the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of issuing authorities, MegaSign, and VeriSign,

• shall not incur liability for representations of information contained in a certificate, provided the certificate content substantially complies with this CPS,

• do not warrant "nonrepudiation" of any certificate or message (because nonrepudiation is determined exclusively by law and the applicable dispute resolution mechanism), and

- do not warrant any software.

IAs, MegaSign, and VeriSign shall not be responsible for nonverified subscriber information (NSI) submitted to MegaSign, an IA, or the MegaSign repository or otherwise submitted for inclusion in a certificate. IAs within the MegaSign Infrastructure will in no event be liable for any damage suffered in case a certificate is used for purposes that do not correspond with certificate-usage as defined in section 1.3.4 of this CPS and the applicable CP.

IAs within the MegaSign Infrastructure will in no event be liable for any damage suffered by a relying party if this relying party has not acted in a manner consistent with the responsibilities as defined in section 2.1.4 of this CPS and the applicable CP.

2.2.1.3 Limitations of liability

2.2.1.3.1 Exclusion of Certain Elements of Damages

IN NO EVENT SHALL ANY ISSUING AUTHORITY, MEGASIGN, OR VERISIGN BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EVEN IF SUCH ISSUING AUTHORITIES, MEGASIGN, OR VERISIGN, OR ANY OR ALL OF THEM, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
INDIRECT DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOST SAVINGS, LOSS OF DATA AND COSTS ASSOCIATED WITH PREVENTING, LIMITING OR DETERMINING DAMAGES.

2.2.1.3.2 Damage and Loss Limitations

IN NO EVENT WILL THE AGGREGATE LIABILITY OF AN ISSUING AUTHORITY AND ALL SUPERIOR IAs IN THE CERTIFICATION CHAIN TO WHICH THE IA's CERTIFICATE BELONGS (AND MEGASIGN AND VERISIGN, AS SPECIFIED) TO ALL PARTIES (INCLUDING WITHOUT LIMITATION A SUBSCRIBER, AN APPLICANT, A RECIPIENT, OR A RELYING PARTY) EXCEED THE APPLICABLE LIABILITY CAP FOR SUCH CERTIFICATE SET FORTH IN TABLE 3, BELOW.

THE COMBINED AGGREGATE LIABILITY OF ALL ISSUING AUTHORITIES, MEGASIGN, AND VERISIGN TO ANY AND ALL PERSONS CONCERNING A SPECIFIC CERTIFICATE SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED THE FOLLOWING, FOR THE AGGREGATE OF ALL DIGITAL SIGNATURES AND TRANSACTIONS RELATED TO SUCH CERTIFICATE:

	LIABILITY CAPS
CLASS 2	$ 5,000.00 US
CLASS 3	$ 100,000.00 US

TABLE 3 - LIABILITY CAPS

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages incurred by any person, including without limitation a subscriber, an applicant, a recipient, or a relying party, that are caused by reliance on or use of a certificate an issuing authority (including any MegaSign or VeriSign IA) issues, manages, uses, suspends or revokes, or such a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall MegaSign or VeriSign be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

2.2.1.4 Applicability

The exclusions in sections 2.2.1.2 and 2.2.1.3 of this CPS shall cease to apply if and insofar as the loss is due to willful intent or gross negligence by MegaSign or another IA within the MegaSign Infrastructure.

2.2.2 RA liability

2.2.2.1 LRA representations to subscribes and relying parties

LRAs make the same representations as IAs in accordance with CPS §§ 2.2.1.1.1-2.2.1.1.2.

2.2.2.2 Disclaimers of warranty

LRAs make the same disclaimers of warranties as IAs do in accordance with CPS §§ 2.2.1.2.

2.2.2.3 Limitations of Liability

LRAs limit their liability as IAs do in accordance with CPS § 2.2.1.3.

2.2.3 Subscribers' liability

By accepting a certificate issued by an IA, the subscriber certifies to and agrees with the IA and to all who reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber,

(i) each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired, suspended or revoked) at the time the digital signature is created,

(ii) no unauthorized person has ever had access to the subscriber's private key,

(iii) all representations made by the subscriber to the IA regarding the information contained in the certificate are true,

(iv) all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and does not promptly notify the IA of any material inaccuracies in such information,

(v) the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and

(vi) the subscriber is an end-user subscriber and not an IA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as an IA or otherwise, unless expressly agreed in writing between subscriber and the IA.

2.3 Financial responsibility

IAs shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to subscribers and recipients of certificates and other persons who may rely on the certificates and time stamps they issue. IAs shall also maintain insurance coverage for errors and omissions.

2.3.1 Indemnification by relying parties

Relying parties shall indemnify MegaSign against all claims by third parties, by whatever name such claims may be known, caused by utilization of certificates inconsistent with the responsibilities laid down in section 2.1.4 of this CPS.

2.3.2 Fiduciary relationships

No IA or RA within the MegaSign infrastructure is the agent, fiduciary, trustee, or other representative of

subscribers or relying parties. The relationship between an IA or RA within the MegaSign infrastructure and subscribers and that between an IA or RA within the MegaSign infrastructure and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind any IA or RA within the MegaSign infrastructure, by contract or otherwise, to any obligation. No IA or RA within the MegaSign infrastructure shall make representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

2.3.3 Administrative processes

An annual report of Roccade can be retrieved by submitting a written request to the address specified in section 1.4.

2.4 Interpretation and Enforcement

2.4.1 Governing law

This CPS, the CPs, the ancillary agreements and any other agreement for the provision of Certification Services within the MegaSign infrastructure are governed by Dutch law.

2.4.2 Severability, survival, merger, notice

a) Severability

In the event that one or more terms, conditions or provisions of this CPS shall be determined for any reason and to any extent invalid, unlawful, or unenforceable, the remainder of this CPS shall not be affected by such finding of invalidity, unlawfulness or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the original intent of the parties.

b) Survival

The obligations and restrictions contained within Section 2.7 (Compliance audit), 2.8 (Confidentiality), 2.1.1 (IA obligations), 2.2.1 (IA liability), 2.2.2 (RA liability), 2.4 (Interpretation and Enforcement) and 2.5.1 (Certification issuance or renewal fees) of this CPS shall survive the termination of this CPS or applicable CPs.

c) Merger

No term or provision of this CPS directly affecting the respective rights and obligations of any party may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or documented of such affected party, except to the extent provided otherwise herein.

d) Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed to the contact-address mentioned in Section 1.4.

2.4.3 Dispute resolution procedures

2.4.3.1 Dispute resolution procedures generally

The procedure follows the subsequent steps:

Before invoking any dispute resolution mechanisms with respect to a dispute involving any aspect of the CPS or any applicable provisions or a certificate issued within the MegaSign infrastructure, aggrieved parties shall notify the issuing IA, and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

In case dispute resolution among themselves is not effective, the dispute shall be resolved by the competent courts in Amsterdam, The Netherlands.

2.4.3.2 Procedures for resolving disputes against VeriSign

Disputes between VeriSign and any non-MegaSign party within the MCS shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) modified as necessary to reflect the provisions herein by one or more arbitrators. The place of arbitration shall be in New York or San Francisco, U.S.A., and the proceedings shall be conducted in English. In cases involving a single arbiter, that single arbiter shall be appointed by mutual agreement of the parties. If the parties fail to agree on an arbiter within fifteen (15) days, the ICC shall choose an arbiter knowledgeable in computer software law, information security, and cryptography or otherwise having special qualifications in the field, such as a lawyer, academician, or judge in a common law jurisdiction.

Nothing in this section shall preclude VeriSign and the applicable IA from seeking equitable (including injunctive) relief upon alleged compromise or alleged material breach in a manner consistent with governing law and this CPS.

2.5 Fees

A general pricing list can be retrieved from the MegaSign repository.

2.5.1 Certificate issuance or renewal fees

MegaSign may charge subscribers for additional services not mentioned in the pricing list.

2.5.2 Certificate access fees

MegaSign may charge subscribers for additional services not mentioned in the pricing list.

2.5.3 Revocation or status information access fees

MegaSign may charge subscribers for additional services not mentioned in the pricing list.

2.5.4 Fees for other services such as policy information

MegaSign may charge subscribers for additional services not mentioned in the pricing list.

2.5.5 Refund policy

If for any reason a subscriber is not completely satisfied with the certificate that was issued to him, her, or it, by an IA within the MegaSign infrastructure, the subscriber may request that this IA revoke the certificate within ***thirty (30)*** days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that the IA revoke the certificate and provide a refund if the IA has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate. After the IA revokes the subscriber's certificate, this IA will promptly credit the subscriber's ***credit card account*** (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via ***common payment means***, for the full amount of the applicable fees paid for the certificate. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

2.6 Publication and Repository

2.6.1 Publication of IA information

Any IA within the MegaSign infrastructure shall make publicly available, in their repositories:

1. this CPS;
2. the CPs;
3. the CRL and other certificate status information;
4. the IA-certificate.

1 and 2 shall also be available in hard-copy against reasonable administration costs.

Any authorized non-MegaSign IA is obliged to communicate the above mentioned information to his own domain only.

2.6.2 Frequency of publication

CPS publication shall be in accordance with Section 2.1.5, 4.4.9 and 8 of this CPS.

2.6.3 Access controls

a) There will be no access control on the reading of this CPS and the CPs it supports.

b) Access controls on certificates, the Certificate Revocation List as well as other certificate status information are optional at the discretion of the IA.

2.6.4 Repositories

The MegaSign repository is (on-line) publicly available for all parties.

7 Compliance audit

Reasons for performing audits on a cyclic basis are to ensure:

- the compliance of the CPS with the CP's;
- the level of trust in the existing CA operations and procedures as stated in the accomplishing CPS.

2.7.1 Frequency of entity compliance audit

Any IA within the MegaSign infrastructure needs to be audited at least once every year.

2.7.2 Identity/qualifications of auditor

The responsible auditor must be familiar with PKI concepts and processes within a CA. In the Netherlands, such an auditor also needs to be certified as a "Register EDP-auditor (RE) by NOREA. The responsible auditor can be assisted by experts who are not a qualified auditor.

2.7.3 Auditor's relationship to audited party

In order to give an impartial and independent statement on the reliability and effectiveness of the CA operations, the external auditor must be sufficiently organizationally separated from the audited party. There cannot exist a conflicting relationship of any kind in order to assure an unbiased evaluation.

2.7.4 Topics covered by audit

The following components of the Certification Services are addressed by the CA audit:

- Primary controls of the CA;
- Key management controls;
- Certificate life-cycle controls.

2.7.5 Actions taken as a result of deficiency

If an audit reveals that an IA's controls are inadequate, the IA shall take steps to remedy the deficiencies and become compliant with the standards against which the audit is performed. If the audited party chooses not to do so and bear the indicated risks, the audit report will include such findings and the superior IA shall determine whether suspension or revocation of the audited IA's certificate is appropriate under CPS § 4.4.1.

2.7.6 Communication of results

Statements regarding the reliability and effectiveness of the CA operations will be communicated to:

- CA being audited;
- Relying parties;
- Subscribers;
- Policy authorities (if applicable).

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

The following information shall be considered confidential information and may not be disclosed, sold nor shared by neither MegaSign nor other IAs within the MegaSign infrastructure, except in those situations as described in the sections 2.8.3 through 2.8.7:
[s1]

1 Subscriber agreements;
2 Certificate application data that is not included in a certificate or repository issued under this CPS;
3 IA application records whether approved or disapproved;
4 transactional records (both full records and the audit trail of transactions);
5 audit trail records created or retained by any IA or RA within the MegaSign infrastructure;
6 audit reports created by VeriSign, MegaSign, a(nother) IA, the VeriSign repository or the MegaSign repository (to the extent such reports are maintained), or their respective auditors (whether internal or public);
7 contingency planning and disaster recovery plans; security measures controlling the operations of IA hardware and software and the administration of certificate services and designated enrollment services;
8 Private keys of subscribers and any IA or RA within the MegaSign infrastructure;
9 tenders;
10 agreements between MegaSign and customers.

2.8.2 Types of information not considered confidential

All information that is not mentioned in Section 2.8.1 shall not be considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

See Section 2.8.2 of this CPS.

2.8.4 Release to law enforcement officials

MegaSign will release information to law enforcement officials if such a release is required according to Dutch laws and/or regulations as well as on a court order.

2.8.5 Release as part of civil discovery

Each end entity has the right to obtain information regarding all data (both confidential as well as non-confidential) relating to him or her that are being processed by any IA or RA within the MegaSign infrastructure against reasonable administrative costs.

2.8.6 Disclosure upon owner's request

Any IA or RA within the MegaSign infrastructure shall disclose confidential data relating to end entities to other parties if a particular end entity explicitly requests for such disclosure.

2.8.7 Other information release circumstances

Not applicable.

2.9 Intellectual Property Rights

The copyrights as well as all other intellectual or industrial property rights to this CPS and other documentation, reports and any preparatory materials belonging thereto, shall exclusively be held by VeriSign.

Breaches of intellectual property rights include, but are not limited to decoding, changing and further distributing of URL-files.

3 Identification and authentication

3.1 Initial Registration

The IA shall confirm that

(a) the certificate applicant is the person identified in the request (in accordance with and only to the extent provided in the certificate class descriptions, *see* CPS § 1.1.1, and as further described below),

(b) the certificate applicant rightfully holds the private key corresponding to the public key to be listed in the certificate (this obligation may be satisfied by a statement to this effect from the certificate applicant, by sending the IA a certificate request message in accordance with PKCS #10, or by another cryptographically equivalent demonstration),

(c) the information to be listed in the certificate is accurate, except for nonverified subscriber information (NSI), and

(d) any agents who apply for a certificate listing the certificate applicant's public key (permissible for Class 3 certificates, for business entities only) are duly authorized to make such a request.

Table 4 (Validation Requirements for Certificate Applications) highlights certain differences between the validation requirements for each certificate class.

VALIDATION REQUIREMENTS	CLASS 2	CLASS 3
PERSONAL PRESENCE	No	Yes – Individuals: Before an IA or LRA (except non-VeriSign organizational LRA applicants) Organizations: Optional
PERSONAL INVESTIGATION (FOR INDIVIDUALS)	No	Yes
THIRD-PARTY AUTOMATED CONFIRMATION OF PERSONAL (INDIVIDUAL) DATA	Under OnSite, no, but otherwise, yes	Yes (*see* description below)
THIRD-PARTY CONFIRMATION OF BUSINESS ENTITIES	N/A	Yes (*see* description below)
POSTAL ADDRESS CONFIRMATION	Yes (*see* below)	N/A
INTERNIC DOMAIN NAME CONFIRMATION	N/A	Yes (*see* description below)

TABLE 4 – VALIDATION REQUIREMENTS FOR CERTIFICATE APPLICATIONS

3.1.1 Types of names

All names used within the MegaSign infrastructure will conform to the X.500 Distinguished Name format.

3.1.2 Need for names to be meaningful

The names that are used within the MegaSign infrastructure are to be defined in such a way that they are meaningful to any entity within the domain in which the names are relied upon. The need for names to be meaningful will not conflict with any law or regulation, including, but not limited to privacy and data protection laws and regulations.

3.1.3 Rules for interpreting various name forms

In case the Organizational Name Attribute as well as the certificate subject attribute are specified in the certificate, this will assume a contractual agreement between the Organization and the certificate subject.

3.1.4 Uniqueness of names

The Names that are issued within the MegaSign infrastructure will uniquely identify a certificate subject.

In the certificate application process, applicant is asked to provide the necessary information for certificate application in accordance with section 3.1.8 and 3.1.9 and accompanying CP's.

The RA will perform an investigation on the uniqueness of the Names that is applied for within the MegaSign infrastructure.

3.1.5 Name claim dispute resolution procedure

In case disputes arise between parties about the use of Names, parties will contact MegaSign. MegaSign will endeavor the utmost to resolve the dispute.

3.1.6 Recognition, authentication and role of trademarks

Applicant/Subscriber bears full responsibility for the legal consequences for the issued names within the MegaSign infrastructure.

MegaSign is not obliged to perform any type of investigation on the existence, the validity or possible infringements of (registered) trademarks that may be part of the Name.

In case of any conflict with respect to the foregoing, the procedure laid down in 3.1.5 applies likewise.

Entities within the MegaSign infrastructure acknowledge that MegaSign will not be part in any conflict with respect to trademarks.

3.1.7 Method to prove possession of private key

End Entities that are issued certificates within the MegaSign infrastructure will prove possession of the associated private key in the following manner.

The proof of possession is realized by signing the certificate request as stipulated in section 4.1 by using the associated private key. A Valid signature verification by the recipient of the certificate request will prove that the associated private key belongs to the sender of the request.

3.1.8 Authentication of organization identity

Validation of Class 3 certificate applications for organizations includes review by the applicable Class 3 IA of authorization records provided by the applicant or third-party business databases, and independent call-backs ("out-of-band" communications) to the organization.

Where required, the third party confirms the business entity's name, address, and other registration information through comparison with third-party databases and through inquiry to the appropriate government entities. Confirmation of information of companies, banks, and their agents requires certain customized (and possibly localized) procedures focusing on specific business-related criteria (such as proper business registration). The third party also provides telephone numbers that are used for out-of-band communications with the business entity to confirm certain information (for example, to confirm an agent's position within the business entity or to confirm that the particular individual listed in the application is in fact the applicant). If its databases do not contain all the information required, the third party may undertake an investigation, if requested by the IA, or the certificate applicant may be required

to provide additional information and proof.

In order to undertake the identification and authentication procedure of organizational entities, MegaSign or any PKI component within the MegaSign infrastructure will use data from a reliable source. The activities of any, by MegaSign, delegated RA will comply with the requirements as set forth in the applicable CP.

The source can be an internal database or it can be a Third Party Data Provider that collects and manages information to be used for business authentication purposes.

The data provider for determining the organizational entity will be periodically evaluated by MegaSign. Additional sources can and will be used for cross verification when applicable.

3.1.9 Authentication of individual identity

The authentication procedure for end entities and the specific documents necessary to prove the identity of the individuals will vary per certificate class.

Details can be found in the applicable CP.

3.1.9.1 Class 2 certificates issued by non-MegaSign organizational LRAs

Certificates issued by non-MegaSign organizational LRAs may only be issued to individuals whose affiliation with the LRA is ascertainable by the LRAA via appropriate internal documentation (such as human relations (HR) employee and independent contractor rolls).

3.1.9.2 Class 3 individual certificates

Individual Class 3 certificate processes utilize various procedures to obtain probative evidence of the identity of individual subscribers. These validation procedures provide stronger assurances of an applicant's identity than Class 2 certificates.

In order to effect an appropriate binding between the applicant and the applicant's public key, individuals applying for Class 3 certificates must appear personally before a trusted entity (such as an LRA) to facilitate the confirmation of their identity. A personal presence requirement may be implemented through the use of well-recognized forms of identification, such as passports and driver's licenses.

3.2 Routine Rekey

Routine Rekey means the generation and installation of a new private key and certificate prior to the existing key pair expiration.

MegaSign will make a reasonable effort via e-mail of the impending expiration of their certificate. Such notice is intended solely for the convenience of the subscriber in the re-enrollment or renewal process, which is applicable.

3.3 Rekey after Revocation

Rekey after revocation means the generation and installation of a new private key and certificate after the revocation of the prior used certificate.

The identification and authentication procedure for the Rekey after revocation procedure will be the same as the procedure for initial registration as defined in section 3.1. There will be no distinction regarding the circumstances for revocation.

3.4 Revocation Request

In case circumstances as specified in section 4.4.1. arise whereby a certificate needs to be revoked, the

entities specified in section 4.4.2 can submit a revocation request.

The identification and authentication of the requester can be determined in the following ways:

- In case the request is performed electronically, the identity of the requester is determined by verifying the digital signature of the requester. This request can also be performed by using the initial challenge phrase which was generated during the application process.
- In case the request is performed physically or by phone, out of band authentication mechanisms will be used.

4 Operational requirements

This chapter describes the foundation and controls for trustworthy MCS operations. It includes the operating requirements for MCS, including record keeping, and auditing requirements. It also presents the obligations of an IA upon the termination of its operations.

4.1 Certificate Application

4.1.1 Certificate Application for End-User Subscriber Certificates

This section describes the certificate application process and lists the certificate application information required for each class of certificate.

In case of an initial application, applicant will sign the necessary contracts and this will bind applicant/subscriber to act in accordance with these contracts, the CPS, the applicable CP's and any regulation declared applicable.

Depending on the certificate type requested, applicant will fill in the specific MegaSign Application Form and provide the necessary information that is required for certificate application. Details of the application procedure are specified in the applicable CP.

Applicant will generate a key pair in accordance with the provisions of section 6 of this CPS and submit a PKCS#10 certificate request to the IA. Applicant will protect the private key of such key pair from compromise.

Identification information provided by the applicant will be verified in accordance with section 3.1.8 or 3.1.9 of this CPS.

The possession of the private key that corresponds to the public key certificate that is being issued will be checked in accordance with the procedure laid down in 3.1.7.

Certificate application information includes the items listed in the following Table 7*. Not all of the following information will appear in a certificate (see* CPS § 7.1.2.7 Figure 4 - Certificates and Information Incorporated by Reference). *Notes*: The items of such information not included in the certificate will be kept confidential by the IA (*see* CPS § 2.8). Certain Class 2 information for affiliated individuals of non-MegaSign organizational LRAs may be not be required in an application but instead made generally available through such LRAs.

CLASS OF CERTIFICATE	REQUIRED CERTIFICATE APPLICATION INFORMATION

CLASS 2	**Individuals:** ***Required Information*** (a) Legal name (in the form of a common name) (b) Proposed distinguished name (c) Street, city, state, postal/zip code, country (of residence) (d) Voice telephone numbers (of residence) (e) E-mail address (f) Subject public key (g) Credit card information (h) Spouse's first name (if applicable) (i) Social security number (j) Date of birth (k) Employer (if applicable) (l) Challenge phrase (to later authenticate subscriber to the IA) (m) Executed subscriber agreement (n) Previous address (if changed within last two years) (o) Driver's license information (if applicable) Other information as prescribed by the IA or MegaSign ***Optional*** (r) Demographic data (Registration Field Information) ***Method of Communicating Application:*** *Same as Class 1.* ***Agents/Authorized Representatives*:** N/A **Business Entities:** Class 2 certificates are issued to individuals only.
CLASS 3	**Individuals:** ***Required Information*** *– Same as Class 2, plus:* (a) Subscriber agreement acknowledged by a notary or LRA (to fulfill the "personal presence" requirement) upon presentation of three (3) forms of identification by the certificate applicant. ***Optional*** – (b) Previous employer ***Agents/Authorized Representative:*** Class 3 permits businesses (but not individuals) to have an agent apply for a certificate, naming the principal (business) as a subscriber. ***Method of Communicating Application*:** TBD **Business Entities**: ***Required Information*** Domain name Organization Organizational unit (if applicable) Technical and billing contact persons City, state, country, postal/zip code (f) Proof of right to use name (via third-party database checks and out-of-band verification) (g) Proof of organizational status (such as proof of articles of incorporation, where applicable, or comparable proof) (h) Proof of agent's authority ***Optional-*** (k) DUNS number ***Agents/Authorized Representative:*** *See above* ***Method of Communicating Application*:** The completed application (and subscriber agreement) shall be submitted in electronic form.

TABLE 7 – REQUIRED CERTIFICATE APPLICATION INFORMATION

4.1.2 Non-MegaSign CA Application

4.1.2.1 Procedure for Application

Each non-MegaSign entity desiring to serve as a subordinate CA shall complete the non-MegaSign CA application applicable to the class of certificate it intends to issue (*inquire of MegaSign for the non-MegaSign CA application form*).

4.1.2.2. Certificate Application Information and Communication

The non-MegaSign CA application will include among other things:

(a) the name, street address, voice and facsimile telephone numbers, and electronic mail address(es) of the CA applicant, its administrative contacts, and its authorized representatives,
(b) the CA applicant's proposed distinguished name,
(c) the CA applicant's public key(s) and the procedures for the generation, storage, use, and destruction of its corresponding private key(s),
(d) a description of any event (for example, current or past insolvency) that could materially affect the CA applicant's ability to act as a subordinate CA pursuant to the CPS,
(e) a reference to, and confirmation of the adoption of, this CPS by the CA applicant and the CA applicant's procedures for distributing copies of this CPS,
(f) a statement of the purpose and scope of anticipated certificate technology, management, or operations to be outsourced,
(g) certified or acknowledged copies of the CA applicant's appropriate business registration documents,
(h) a representation by the CA applicant that to its best knowledge and belief it can and will comply with the requirements of this CPS, and
(i) any other information required by MegaSign.

CA applications must be acknowledged before a notary. Failure by a CA applicant to provide the required information will delay or preclude CA application processing.

Completed, notarially acknowledged CA applications (including required supplemental information) shall be submitted to the applicable MegaSign CA at:

MegaSign
PO Box 9105
7300 HN APELDOORN

4.1.3 Change of Subscriber Information Maintained by an IA

Any subscriber may change certain information about itself on file with its IA that does not appear within its certificate (typically, information provided in the subscriber agreement or certificate application) upon giving thirty (30) days notice in accordance with CPS § 2.4.2.4 (Notice). Such change in information shall be effective after such thirty (30) day period.

4.2 Certificate Issuance and Rejection of Certificate Applications

4.2.1 End-User Subscriber Certificates

4.2.1.1 Issuance of End-User Subscriber Certificates

After the procedures laid down in 4.1 have been completed and upon successful validations of a certificate application (in accordance with CPS § 3.1), the CA will approve the application. Approval is demonstrated by issuing a certificate that binds the public key to the information as provided by the applicant. The certificate is deemed to be a valid certificate upon the subscriber's acceptance of it (*see* CPS § 4.3 regarding acceptance).

Subscriber and, if applicable, CA Administrator, will be notified of certificate issuance. The subscriber is informed about the details of certificate retrieval and installation.

The certificate can be retrieved and installed by the Subscriber after authentication by means of a passphrase, via a secured connection.

4.2.1.2 Rejection of Certificate Applications for End-User Subscriber Certificates

If a validation fails, the applicable IA shall reject the certificate application by promptly notifying the certificate applicant of the validation failure and providing the reason code (except where prohibited by law) for such failure. Where such validation failure is caused as a result of third-party database information, the applicable IA shall provide the certificate applicant with the third-party database company's contact information for inquiry and dispute resolution. Such notice shall be communicated to the certificate applicant using the same method as was used to communicate the certificate application to the IA (or LRA).

A person whose certificate application has been rejected may thereafter reapply.

An IA may refuse to issue a certificate to any person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Upon an IA's refusal to issue a certificate, the IA shall promptly refund to any certificate applicant any paid certificate enrollment fee, unless the certificate applicant submitted fraudulent or falsified information to the IA.

4.2.2 Non-MegaSign CA Applications

4.2.2.1 Approval to Initiate CA Activities

Upon completion of its review of a CA application and the performance of such further investigation as it shall deem appropriate, the applicable MegaSign CA shall approve or deny the CA applicant's participation as a subordinate CA. The applicable MegaSign CA shall make a reasonable effort to approve or deny such applications within three to six business weeks.

MegaSign will indicate its approval of a CA application by (i) executing a MegaSign-CA agreement and (ii) issuing a certificate to the applicant. The decision to approve or deny a CA application shall be solely at the discretion of the applicable MegaSign CA, which further reserves the right to rescind subordinate CA approval at any time. Breach of or failure to observe CPS requirements is reasonable basis for rescission.

4.2.2.2 Conformance to Operational Period Constraints

The CA applicant shall ensure that the operational period assigned to an IA certificate conforms to the restrictions imposed on that IA by the superior IA that establishes operational periods.

4.3 Certificate Acceptance

The passphrase, that is used to retrieve the certificate, is strictly personal and is therefore to be kept confidential by the subscriber.

The certificate is deemed accepted by the subscriber when the certificate has been retrieved by using the passphrase that has been provided exclusively to the subscriber. Note: : The certificate applicant must notify the IA of any inaccuracy or defect in a certificate promptly after receipt of the certificate or publication of the certificate in the repository, or upon earlier notice of informational content to be included in the certificate.

A subscriber must not create digital signatures using a private key corresponding to the public key listed in a certificate (or otherwise use such private key) if the foreseeable effect would be to induce or allow reliance upon a certificate which is invalid (because it has not been accepted).

Upon acceptation, the certificate is published in the MegaSign repository.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

4.4.1.1 Generally

A certificate shall be suspended or revoked if

- there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject,
- the certificate's subject (whether an IA or a subscriber) has breached a material obligation under this CPS, or
- the performance of a person's obligations under this CPS is delayed or prevented by an act of God; natural disaster; computer or communications failure; change in statute, regulation, or other law; official government action, including but not limited to acts by agencies responsible for export control administration; or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.

4.4.1.2 Revocation of an IA's Certificate

An IA must make a reasonable effort to suspend or revoke a subordinate IA's certificate, regardless of whether the subordinate IA consents, if it determines any of the following:

- a material fact represented in the certificate is known or reasonably believed by the IA to be false,
- a material prerequisite to certificate issuance was neither satisfied nor waived,
- the subordinate IA's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability, or
- the certificate's subject (here, an IA) has breached a material obligation under this CPS.

The IA must promptly notify the subordinate IA of any such suspension or revocation.

4.4.1.3 Revocation at Subscriber's Request

An IA must revoke a certificate upon the subscriber's request once it has confirmed that the person requesting the revocation is in fact the subscriber.

4.4.1.4 Revocation Due to Faulty Issuance

An IA shall revoke a certificate promptly upon discovering and confirming that it was not issued in accordance with the procedures required by this CPS. A certificate may be suspended while the IA investigates to confirm grounds for revocation. Table 9 details revocation prerequisites.

	PREREQUISITES FOR AN IA REVOKING A CERTIFICATE
VR	• N/A
PCA AND CA	• Certificate revocation request from a subordinate IA. • Request in the form of an authenticated record or voice message from the subscriber or its agent, authenticated by means of a challenge phrase or recitation of certain presubmitted enrollment information.

TABLE 9 – REVOCATION PREREQUISITES

4.4.2 Who can request revocation

The following entities can request revocation:

- Subscriber
- The IA that issued the certificate

- The LRA that approved the certificate application.

4.4.3 Procedure for revocation request

The entities specified in 4.4.2 may request that the IA revoke the certificate using the identification and authentication methods which are specified in section 3.4 of this CPS.

Only the IA can perform the revocation procedure. After compliance with the circumstances as set forth in 4.4.1, the certificate shall be revoked by the IA. Upon revocation, the certificate will be published in the CRL and the fact of the revocation shall be published in the repository.

4.4.4 Revocation request grace period

Upon the receipt of a revocation request, MegaSign shall undertake to perform the revocation procedure as soon as possible.

4.4.5 Circumstances for suspension

Suspension is currently not available for end user subscriber certificates. MegaSign will offer this service at a later time. With respect to circumstances for suspension of an IA's certificate, the following provisions apply. An IA shall suspend a subordinate IA's certificate upon the request of a duly authorized representative of the subordinate IA or of a person claiming to be the subordinate IA or a person in a position likely to know of a compromise of the subordinate IA's private key, such as an agent or employee of the subordinate IA. *See also* section 4.4.1.2. Such suspension must be undertaken in accordance with the suspension prerequisites stated in Table 10 as follows.

	PREREQUISITES FOR SUSPENDING AN IA'S CERTIFICATE
VR	• N/A
PCA AND CA	• Request from subordinate IA. • Request in the form of an authenticated record or a fax or voice message from the subscriber or its agent (authenticated by means of a challenge phrase or recitation of certain presubmitted enrollment information). **Note:** The IA need not further confirm the identity or agency of the person requesting such a suspension. An IA that suspends a subordinate IA's certificate in accordance with CPS § 4.4.5.1.3 shall not be held liable for the unauthorized suspension of such certificate provided that it acts in good faith upon purportedly authorized instructions.

TABLE 10 – SUSPENSION PREREQUISITES

4.4.6 Who can request suspension

Suspension is currently not available for end user subscriber certificates. MegaSign will offer this service at a later time. With respect to suspension of an IA's certificate, see section 4.4.5.

4.4.7 Procedure for suspension request

See section 4.4.3. The same procedure applies as revocation requests, but may result in certificate suspension.

4.4.8 Limits on suspension period

There are no limits on the suspension period. Suspension may be terminated. Upon certificate suspension, the subscriber may at any time submit a revocation request in accordance with 4.4.3 in order to terminate

the suspension.

In addition, an IA shall terminate a certificate suspension (thereby reinstating the certificate), if (i) the subscriber requests it and the IA confirms his or her identity, (ii) the IA determines that the request for suspension was made without the suspended IA's authorization, or (iii) the IA determines that the reasons for the suspension were unfounded.

4.4.9 CRL issuance frequency (if applicable)

The issuance frequency of the CRL may vary per certificate type and has therefore been specified in the applicable CP. The minimum CRL issuance frequency is set to once per 24 hours. Additional services can be offered on request. CRLs shall also be issued on an emergency basis, as determined by the IA.

4.4.10 CRL checking requirements

The recipient of a certificate must determine if any of the certificates along the chain from end-user subscriber to an acceptable root within the MCS has been revoked or suspended. Each relying party is responsible for checking the CRL and will get information on the revocation status of the certificate. The MCS CRL can be accessed by use of appropriate software via different protocols such as LDAP and http.

4.4.11 On-line revocation/status checking availability

On-line revocation status checking is supported via OCSP. In addition, relying parties can determine the status of a certificate by checking the repository.

4.4.12 On-line revocation checking requirements

On-line revocation checking needs to be supported by client applications like mail or web browsers.

4.4.13 Other forms of revocation advertisements available

Any entity within the MegaSign infrastructure can contact MegaSign in order to check the validity of public available certificates.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulations..

4.4.15 Special requirements re key compromise

In case of re key compromise, the procedure laid down in 4.4.3. is likewise applicable.

Accordingly:
- subscriber is notified of revocation upon the repetitive key compromise;
- in the event that key compromise occurred due to security failures, MegaSign will take appropriate measures to prevent these occurrences in the future.

In case of multiple re-key compromise by a subscriber within one year, MegaSign reserves the right to terminate the contract with such subscriber or to terminate service offerings to this subscriber, if MegaSign determines that future activity of such subscriber constitutes a material risk to the trustworthiness of the MCS and/or VeriSign Trust Network.

4.5 Security Audit Procedures

4.5.1 Types of event recorded

There are two type of logfiles:

- 1) IT systems logfiles upon the occurrence of certain events, including but not limited to:
  - startup/shutdown system;
  - recording user accounts;
  - backup information;
  - logfiles information;
  - tasks performed by any application;
  - tasks performed by any user.

- 2) TTP logfiles (upon the occurrence of certain events, including but not limited to)
  - the creation LDIF files to be imported in LDAP directory;
  - transaction request;
  - transaction status.

  These logfiles are regularly backuped and stored off-line and off-site.

  4.5.2 Frequency of processing log

  The processing of the logfiles is on-line. Matters that need attention are mail to three different mailboxes dependent on the severity of the error and /or importance of the information.

-

  4.5.3 Retention period for audit log

  The period for retaining the audit logs is in accordance with section 4.6.2. The retention period of data published in the LDAP directory and archived data is 5 years for Class 2 certificates and 30 years for Class 3 certificates..

  4.5.4 Protection of audit log

- Audit logs created by MegaSign are (cryptographically) signed. Only Audit personnel of MegaSign are allowed to process these files.

  4.5.5 Audit log backup procedures

-
- Onsite backup with physical removal and storage every week in an outside location, which is protected with similar security level measures as the principal location

  4.5.6 Audit collection system (internal vs external)

  MegaSign uses both collection systems

  4.5.7 Notification to event-causing subject

  Matters that need attention are mail to different mailboxes dependent on the severity of the error and /or importance of the information.

  4.5.8 Vulnerability assessments

  The audit logs are analyzed by Operations. In case of any deficiency, operators will try to solve the incidents according to the well-defined procedure. Matters that need attention are mail to different mailboxes dependent on the severity of the error and /or importance of the information.

4.6 Records Archival

a) Records documenting compliance

IAs shall maintain and make available to MegaSign upon request, records in a trustworthy fashion,

including

(i) documentation of their own compliance with the CPS, and

(ii) documentation of actions and information that is material to each certificate application and to the creation, issuance, use, suspension, revocation, expiration, and renewal or re-enrollment of each certificate it issues. These records shall include all relevant evidence in the IA's possession regarding

- the identity of the subscriber named in each certificate (except for Class 1 certificates, for which only a record of the subscriber's unambiguous name is maintained),
- the identity of persons requesting certificate suspension or revocation (except for Class 1 certificates, for which only a record of the subscriber's unambiguous name is maintained),
- other facts represented in the certificate,
- time stamps, and
- certain foreseeable material facts related to issuing certificates.

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete. An IA may require a subscriber or its agent to submit documents to enable the IA to comply with this section.

4.6.1 Types of event recorded

No stipulations.

4.6.2 Retention period for archive

Records Retention Schedule

IAs shall retain in a trustworthy fashion records associated with Class 1 and 2 certificates for at least five (5) years and records associated with Class 3 certificates for at least thirty (30) years after the date a certificate is revoked or expires. Such records may be retained as either retrievable computer-based messages or paper-based documents.

4.6.3 Protection of archive

No stipulations.

4.6.4 Archive backup procedures

MegaSign has a separate off-site archive backup storage for documents and media. The location of the separate off-site backup storage is not the same as the location of Roccade Megaplex TTP services.

4.6.5 Requirements for time-stamping of records

The TTP services will use unique and accurate time-stamping methods.

4.6.6 Archive collection system (internal or external)

MegaSign uses both collection systems.

4.6.7 Procedures to obtain and verify archive information

No stipulations.

4.7 Key changeover

No stipulations.

4.8 Compromise and Disaster Recovery

a) Contingency Planning and Disaster Recovery

IAs shall implement, document, and periodically test appropriate contingency planning and disaster recovery capabilities and procedures, consistent with this CPS and the VSP.

b) MegaSign's Right to Investigate Compromises

IAs, VeriSign, and MegaSign may, but are not obligated to, investigate all compromises to the furthest extent of the law. By submitting a CA application (*see* CPS § 4.1.2) or certificate application (*see* CPS § 4.1.1), all applicants authorize the undertaking and scope of such investigations and agree to assist in determining all facts, circumstances, and other pertinent information that the IA, VeriSign, and/or MegaSign deem appropriate and consistent with the CPS, provided that such investigations comply with all applicable privacy and data protection laws. Investigations of IAs may include but are not necessarily limited to interviews, the review of applicable books, records, and procedures, and the examination and inspection of relevant facilities. Investigations of certificate applicants and subscribers may include but are not necessarily limited to interviews and requests for and evaluation of documents.

4.8.1 Computing resources, software, and/or data are corrupted

No stipulations.

4.8.2 Entity public key is revoked

No stipulations.

4.8.3 Entity key is compromised

No stipulations.

4.8.4 Secure facility after a natural or other type of disaster

No stipulations.

4.9 Termination

The following obligations are intended to reduce the impact of a termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, and certain remedies.

4.9.1 Requirements Prior to Cessation

Before ceasing to act as an IA, an IA must:

(i) Notify MegaSign of its intention to cease acting as an IA. Such notice shall be made at least ninety (90) days before ceasing to act as an IA. The superior IA may require additional statements in order to verify compliance with this provision (MegaSign will also notify VeriSign of the IA's intention to cease acting as an IA).

(ii) Provide to the subscriber of each unrevoked or unexpired certificate it issued ninety (90) days notice of its intention to cease acting as an IA.

(iii) Revoke all certificates that remain unrevoked or unexpired at the end of the ninety (90) day notice period, whether or not the subscribers have requested revocation.

(iv) Give notice of revocation to each affected subscriber, as detailed in CPS § 2.1.1.4.

(v) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding certificates.

(vi) Make reasonable arrangements for preserving its records.

(vii) Pay reasonable restitution (not to exceed the certificate purchase price) to subscribers for revoking

their certificates before their expiration date.

4.9.2 Reissuance of Certificates by a Successor IA

To provide uninterrupted IA services to its certificate applicants and subscribers, a discontinuing IA must arrange with another such authority, subject to the other IA's prior written approval, for reissuance of its outstanding subscriber certificates. In reissuing a certificate, the succeeding IA (not to be confused with a subordinate IA) is subrogated to the rights and defenses of the discontinuing IA and, to the extent agreed in writing between the discontinuing and succeeding IA, assumes all of its obligations and liabilities regarding outstanding certificates. Unless a contract between the discontinuing IA and a subscriber provides otherwise, and subject to the succeeding IA's written approval, the CPS will remain in effect under the succeeding IA as under the original IA.

The requirements of this subsection may be varied by contract, provided such modifications affect only the contracting parties.

4.10 Time Stamping

Time stamping is intended to enhance the integrity of MegaSign's MCS and the trustworthiness of certificates and to contribute to the nonrepudiation of digitally signed messages. Time stamping creates a notation that indicates (at least) the correct date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation. All time stamps reflect Greenwich mean time (GMT) and adopt the Universal Time Conventions (UTC). For purposes of this CPS, any two-digit year in the range 00-69 means 2000-2069, and in the range 70-99 means 1970-1999.

The following data shall be time stamped, either directly on the data or on a correspondingly trustworthy audit trail, by the applicable IAs:

- certificates,
- CRLs and other suspension and revocation database entries,
- each version of the CPS,
- customer service messages, and
- other information, as prescribed by this CPS.

Note: *Cryptographic-based time stamping is not currently utilized by MCS IAs. It will be incrementally implemented by MegaSign IAs for all relevant messages.*

5 Physical, procedural and personnel security controls

This chapter describes the attributes of the physical, procedural and personnel security controls. These measures are necessary to protect the trust and integrity of the business assets that are used for the MCS.

5.1 Physical Controls

An IA shall operate trustworthy facilities that are in substantial conformance with the MSP, or equivalent. More specifically, with respect to MegaSign, the physical controls are based on a multi layer structure. This structure is divided into two categories
1) the first layers are protecting the Megaplex facility;
2) the second layers are protecting the key management environment.

5.1.1 Site location and construction

The Megaplex facility, which accommodates the MCS, is located in the city of Apeldoorn, the Netherlands. The physical controls consist of procedural and technical measures. The building has constructional measures to protect the building against unauthorized access. The access to the building and critical environments are additionally protected with electronic devices and visual control.

The site location of the MCS consists of separated physical environments.

5.1.2 Physical access

The physical access system incorporates measures for registration of entrance- and exit time for personal. The surveillance systems automatically detect and registrar attempts of unauthorized access.

The computer- and network equipment for the CA operation facility is placed in a separate environment within the computing center. The MCS environments can only be accessed by authorized personnel. Physical access and authorization for the separate environments are controlled by state-of-the-art biometrics-based technology.

5.1.3 Power and air conditioning

The MCS environment is protected against power outage by means of own power generation facilities, continuous air conditioning to ensure maximum security and reliability.

5.1.4 Water exposures

No water supply is present on the computing center. There is a separate water drainage system available for external water exposures.

5.1.5 Fire prevention and protection

The MCS environment has a fire prevention, detection and protection installation to meet security and safety measures at the premises.

5.1.6 Media storage

The MCS environment has a secure media and paper storage on the site location. The tape and media handling procedures (e.g. for back-up purposes) are in accordance with well defined procedures.

5.1.7 Waste disposal

The MCS environment has a separate waste disposal and secure destruction for media and paper.

5.1.8 Off-site backup

The MCS environment has a separate off-site backup storage for documents and media. The location of the separate off-site backup storage is not the same as the location of the MCS environment in the city of Apeldoorn, the Netherlands.

5.2 Procedural Controls

The procedural controls are based on the Information Technology Infrastructure Library (ITIL), with the following management areas: Service, Availability, Capacity, Customer Service desk, Incident, Problem, Change, Security, Configuration, Operations and Contingency.

5.2.1 Trusted roles

In general, all employees, contractors, and consultants of an IA (collectively, "personnel") that have access to or control over cryptographic operations that may materially affect the IA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the MegaSign repository, shall, for purposes of this CPS, be considered as serving in a trusted position. Such personnel include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel, and executives who are designated to oversee the IA's trustworthy system infrastructures. More specifically, for the three areas noted below, the trusted roles are as follows:

1) System Administration and associated tasks like:
- ITIL system management of the Information Systems (IT)
- User management of the IT systems
- Creation of backup of IT systems
- Performing software upgrades and recovery
- Distribution of the backups.

- 2) CA management and associated tasks like:
  - Certificate generation and distributing
  - Key management
  - Database management

3) Security Management and associated tasks like:
- Deploying and maintaining security policy
- Deploying and maintaining trusted employee policy
- Review of audit logging

In addition, LRAAs serve in trusted positions.

5.2.2 Number of persons required per task

Because of security reasons this CPS makes no stipulation on number of persons required per task with the exception that the number of persons required per task is based on separation of duties.

5.2.3 Identification and authentication for each role

The identification and authentication for each role of System Administration, CA Administration, and Security Management shall be appropriate and consistent with practices, procedures and conditions stated in this CPS. For all trusted employees of the MCS a background check is done by the National Security Service of the Ministry of the Interior in accordance with section 5.3.2.

5.3 Personnel Controls

The trustworthiness and reliability of any IA within the MegaSign infrastructure depends, among other things, on the integrity of staff members. MegaSign, as a part of Roccade Megaplex, defines integrity in the context of this section as honesty, reliability and incorruptibility. Additionally Roccade Megaplex is appointed as a company of vital importance by the government of the Netherlands. This invokes additional obligations which are also included in this section.

IAs within the MegaSign infrastructure shall formulate and follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. Such practices shall be consistent with this CPS.

5.3.1 Background, qualifications, experience, and clearance requirements

IAs shall conduct an initial investigation of all personnel who are candidates to serve in trusted positions to make a reasonable attempt to determine their trustworthiness and competence. All personnel serving in trusted positions shall be accredited by a recognized external accreditation organization, as appropriate. This provision does not include members of the board of directors of MegaSign or of any IA, except for such persons serving in an operational capacity in the PCS.

Every applicant for a function in the Roccade Megaplex or MegaSign organization is required to submit his or her passport to Roccade Megaplex in order to check personal details and nationality. Qualifications are verified against diplomas. Work experience must be justified using publications, personal references or other documents. Finally every individual must have a so-called "proof of good behavior" in order to be working in the MegaSign organization.
The minimum requirements for an LRAA and IA personnel performing validation functions depend upon the class and affiliation of the certificates issued, based on the applications that an LRAA is authorized to approve. Note that certain non-MegaSign organizational LRA requirements are less rigorous than requirements for a normal LRAA because the former does not issue certificates to the general public and therefore requires less experience in the general validation of identification documents. Rather, the non-MegaSign organizational LRA bases its certificate approval decisions upon a simplified, internal list of authorized employees and other "affiliates" or other business records.

5.3.2 Background check procedures

IAs shall conduct periodic investigations of all personnel who serve in trusted positions to verify their continued trustworthiness and competence in accordance with MegaSign's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve in a trusted position. The removal of any person serving in a trusted position shall be at the sole discretion of the applicable IA (or MegaSign, in the case of MegaSign personnel).

Roccade Megaplex is considered a company of vital importance by the government of the Netherlands. Therefore special demands for background checking are in place for all personal who have a trusted role within Roccade Megaplex and the MCS organization. These background checks are performed in accordance with the Dutch Security Investigations Act. All background checks are done by the Dutch National Security Service of the Ministry of Home Affairs. For all other personnel of Roccade Megaplex a proof of good behavior is obligatory. Such security investigations are carried out on a regularly basis (once every 5 years).

5.3.3 Training requirements

All personnel within the MCS environment are appropriately trained for the fulfillment of their role and tasks. See section 5.3.1.

5.3.4 Retraining frequency and requirements

When there are changes regarding the enforcement of MegaSign's CA operations, personnel shall be made aware of the forthcoming changes and their effect on the provision of Certification Services by MegaSign.

In case of *major changes* regarding the Certification Services, MegaSign provides its personnel with adequate training and documentation. Examples of major changes are: software or hardware upgrade, key management or security changes.

In case of *minor changes* regarding the Certification Services, MegaSign only provides information to its personnel.

All change management procedures are conducted conforming ITIL standards.

5.3.5 Job rotation frequency and sequence

Job rotation of personnel does not affect the continuity and integrity of the MCS.

5.3.6 Sanctions for unauthorized actions

All personnel, including personnel of third-party contractors, are obliged to sign a non-disclosure agreement and to act in accordance with applicable procedures (e.g. company regulations). This agreement and procedures state the sanctions in case of any violations.

If personnel do not act in accordance with the above-stipulated measures, whether through negligence or with malicious intent, privileges may be revoked and personnel may be subjected to administrative discipline (e.g. discharge) and reported to official authorities (e.g. police department).

5.3.7 Contracting personnel requirements

Roccade works with 'preferred suppliers' to contract personnel. Roccade Megaplex and the preferred suppliers always sign a framework agreement. The preferred suppliers have declared that they agree with the Roccade Megaplex security policy. For all contracting personnel the same background check is performed as mentioned in section 5.3.2. There is also a so called "black list" of companies available. It is prohibited for MegaSign to do business with any of companies listed by Roccade Megaplex on the "black list."

5.3.8 Documentation supplied to personnel

The security policy is generally available for all personnel. All personnel receive updates of the security policy through announcements and publications.

6 Technical security controls

a) Use of trustworthy systems

IAs, LRAs, and the MegaSign repository shall utilize only trustworthy systems in performing their respective services.

b) Communications security requirements

All communications pursuant to this CPS among MegaSign and the other parties in the MCS must use systems that provide appropriate security mechanisms commensurate with the attendant risks. Without limiting the generality of the foregoing, computer-based notices, corresponding notice acknowledgments, and any other communications affecting the security of the MCS shall also be appropriately secured.

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The Roccade Megaplex TTP services shall securely generate and protect its own private key(s), using a trustworthy system, and take necessary precautions to prevent its loss, disclosure, modification, or unauthorized use.

6.1.2 Private key delivery to entity

No stipulations.

6.1.3 Public key delivery to certificate issuer

No stipulations.

6.1.4 CA public key delivery to users

MegaSign has its own root, can potentially be trusted based upon out-of-band authentication mechanisms.

6.1.5 Key sizes

The MegaSign Root is signing each initial ID with a key size of 1024 bits.

6.1.6 Public key parameters generation

No stipulations.

6.1.7 Parameter quality checking

No stipulations.

6.1.8 Hardware/software key generation

A trustworthy hardware device (FIPS 140-1 Level 2 certified) is used to create, protect, and destroy the private keys of Class 2, and 3 CAs.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

No stipulations.

6.2 Private Key Protection

a) End-user subscriber private key protection

The secrecy of the private keys of certificate subscribers (and applicants) must be protected through the use of encryption software or hardware tokens (such as smart cards or PC cards) as specified in this CPS. *See* CPS § 2.1.4.2 (Key Generation and Protection) and the Key Protection FAQ at **https://www.MegaSign.nl**

b) IA private key protection

IAs must use approved trustworthy hardware cryptomodules for all operations requiring the use of their private key. The procedure for creating such private keys may be published in the repository.

6.2.1 Standards for cryptographic module

A trustworthy hardware device (FIPS 140-1 Level 2 certified) is used to create, protect, and destroy the MR's private key, each PCA's private key, and the private keys of Class 2 and 3 CAs.

6.2.2 Private key (n out of m) multi-person control

No stipulations.

6.2.3 Private key escrow

No stipulations.

6.2.4 Private key backup

No stipulations.

6.2.5 Private key archival

No stipulations.

6.2.6 Private key entry into cryptographic module

No stipulations.

6.2.7 Method of activating private key

No stipulations.

6.2.8 Method of deactivating private key

No stipulations.

6.2.9 Method of destroying private key

No stipulations.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

No stipulations.

6.3.2 Usage periods for the public and private keys

All certificates shall be considered valid upon issuance by the applicable IA and acceptance by the subscriber . The standard operational periods for the various classes of certificates are as follows, subject to earlier termination of the operational period due to suspension or revocation.

CERTIFICATE ISSUED BY:	CLASS 2		CLASS 3
VR OR PCA TO PCA	10 years		10 years
PCA TO CA	5 years		5 years
CA TO SUBORDINATE CA	5 years		5 years
CA TO END-USER/ SUBSCRIBER	Pro-visional Cert.: 21 days	Norm. Cert.: 1 year	1 year

TABLE 13 – CERTIFICATE OPERATIONAL

All certificates begin their operational period at the date and time of issuance, unless a later date and time (no later than sixty (60) days after the date of issue) is indicated in the certificate. The operational period begins at this date and time even if the certificate has not yet been accepted and is therefore not yet valid.

6.4 Activation Data

6.4.1 Activation data generation and installation

No stipulations.

6.4.2 Activation data protection

No stipulations.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer Security Controls

Roccade Megaplex TTP services shall utilize only trustworthy systems for the TTP services.

6.5.1 Specific computer security technical requirements

No stipulations.

6.5.2 Computer security rating

No stipulations.

6.6 Life Cycle Technical Controls

Roccade Megaplex TTP services shall utilize only trustworthy systems for the TTP services.

6.6.1 System development controls

No stipulations.

6.6.2 Security management controls

No stipulations.

6.6.3 Life cycle security ratings

No stipulations.

6.7 Network Security Controls

The network for Roccade Megaplex TTP service is a dedicated production environment with only access from the Internet.

6.8 Cryptographic Module Engineering Controls

No stipulations.

7 Certificate and CRL profiles

7.1 Certificate Profile

7.1.1 Version number(s)

The MegaSign Certification Services facilitates the use of X.509 version 1, 2 and 3 certificates. The X.509 v3 certificates expand the capabilities of v1 and v2, including the ability to add certificate extensions. This capability, a standard component of MegaSign's Certification Services, augments the standard authentication services model.

7.1.2 Certificate extensions

The certificate extensions and the X.509 certificate profile can be retrieved from the MegaSign repository.

a) Standard and Service-Specific Extensions

The X.509 "Amendment 1 to ISO/IEC 9594-8:1995" defines a number of extensions. These provide various management and administrative controls useful for large-scale and multipurpose authentication. MegaSign exploits a number of these controls for the purposes intended by X.509.

(Note: X.509-compliant user software is assumed to enforce the validation requirements of this CPS. Issuing Authorities and MegaSign cannot guarantee that such software will support and enforce these controls.)

In addition, this CPS allows users to define additional "private" extensions for purposes or modes of use specific to their application environment. Definitions for service-oriented extensions to and practices for handling such information during certificate application, approval, and issuance, are specified in the MegaSign accompanying CP's.

Examples of private extensions implemented within the MCS for service-specific purposes include the software validation scheme exploited by some versions of Microsoft Windows® software and the Netscape Communications Corporation's scheme for SSL security technology.

See http://microsoft.com/security, and http://home.netscape.com/newsref/ref/netscape-security.html.

b) Identification and Criticality of Specific Extensions

The function of each extension is indicated by a standard OBJECT IDENTIFIER value (*see* definition for X.509). Additionally, each extension in a certificate is assigned a "criticality" true/false value. This value is set by the Issuing Authority, possibly on the basis of information provided by the certificate applicant on the certificate application. This value must conform to certain constraints imposed by the organization responsible for the extension definition.

The presence of a criticality value of *true* upon a specific extension requires all persons validating the certificate to consider the certificate invalid if they lack knowledge of the purposes and handling requirements for any specific extension with criticality value of *true*. If the criticality value of such extension is *false*, all persons shall process the extension in conformance with the applicable definition when performing validation or else ignore the extension.

c) End-User Subscriber Certificate Extensions

Issuing Authorities serving end-user subscribers may issue certificates containing extensions defined both by the X.509 Amendment 1 to ISO/IEC 9594-8:1995 and by sponsoring organizations such as Microsoft and Netscape (*see* item a).

ISO-defined extensions used in the MegaSign infrastructure, whose content is assigned by the applicable Issuing Authority , are currently limited to the following extensions:

- basic constraints,
- key usage, and
- certificate policy.

Briefly, the use of these extensions control the process of issuing and validating certificates. Table 14 in item g describes which extensions are present in particular certificates.

d) ISO-Defined Basic Constraints Extension

The basic constraints extension serves to delimit the role and position an Issuing Authority or end-user subscriber certificate plays in a chain of certificates. For example, certificates issued to CAs and subordinate CAs contain a basic constraint extension that identifies them as Issuing Authority Certificates. End-user Subscriber Certificates contain an extension that constrains the certificate from being an Issuing Authority Certificate.

e) ISO-Defined Key Usage Extension

The key usage extension serves to limit the technical purposes for which a public key listed in a valid certificate may be used within the MCS. Issuing Authority Certificates may contain a key usage extension that restricts the key to signing certificates, certificate revocation lists, and other data.

f) ISO-Defined Certificate Policy Extension

The certificate policy extension limits a certificate to the practices required by (or indicated to) relying parties. The certificate policy extension, as implemented in the MCS, points its users to the appropriate CP and qualifies appropriate usage's (*See also* item g in this section).

g) Policy Information Generally

When digital signature-verifying software or hardware (collectively, "verifying software") facilitates the acceptance and use of v3 certificate extensions, the verifying software will display both a reference to the CPS and a set of extensions that describe important portions of it. If the verifying software supports only limited or privately defined v3 extensions, the verifying software may then make use of those application-specific extensions, as appropriate, to equivalently disclose certain critical practice statement sections.

Figure 4 illustrates how MegaSign has implemented this approach within v3 certificates. Key elements in the figure are explained below.

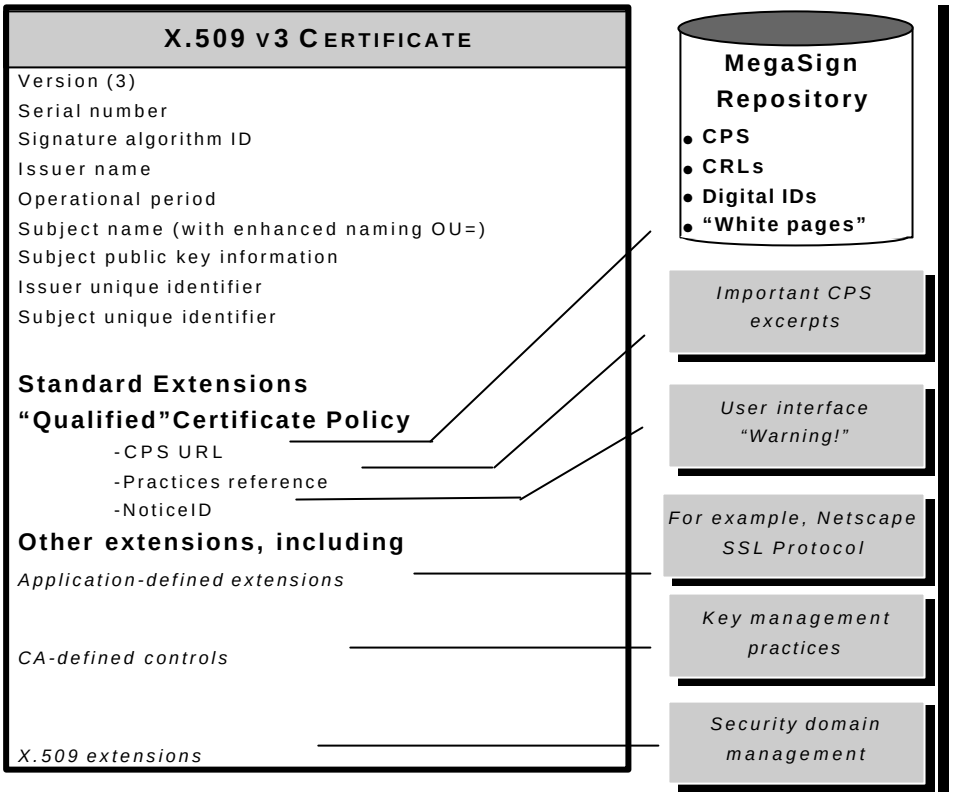

Figure 4 – Certificates and information incorporated by reference

g1) Incorporation by Reference

Extensions and enhanced naming are either fully expressed within a certificate or they are at least partially expressed in a certificate with the balance expressed in an external document incorporated by reference in the certificate.
(to make one message a part of another message by identifying the message to be incorporated, with information that enables the receiving party to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message to the extent permitted by law.)

The information contained in the enhanced Organizational Unit field is also present in the **certificatePolicy** extension, when present in a certificate. This CPS constitutes a "certificate policy" as defined by X.509 Amendment 1 to ISO/IEC 9594-8:1995.

MegaSign, acting as a policy-defining authority, has assigned to the CPS an object identifier value which is present in the **certificatePolicy** extension. The definition of this "certificate policy" requires the use of a policy qualifier which MegaSign has defined to include pointer values, warnings, liability limitations, and warranty disclaimers as described in section g3.

g2) Pointers to CPS

Both computer-based pointers (using URLs or other identifiers and mechanisms) and English (human-readable) text or pointers are used, so that certificate users can easily locate and access the CPS and other relevant information.

g3) Warnings, Liability Limitations, and Warranty Disclaimers

Each certificate includes a brief statement detailing applicable limitations of liability and disclaimers of warranty, with a pointer to the full text of such warnings, limitations, and disclaimers in the CPS. Alternatively, such information may be displayed by a certificate-viewing function, possibly following a hypertext link to a message accessible by users or agents, rather than being embedded in the certificate.

The methods of communicating information (to be displayed by a user) are as follows: an enhanced naming organizational unit attribute; a MegaSign standard qualifier to a MegaSign–registered certificate policy (using a standard v3 extension); and other vendors' registered extensions (such as a Netscape–registered "Comment" extension).

An "enhanced" organizational unit attribute contains the string:

"**OU= www.megasign.nl/repository/CPS**", or similar string.

Table 14 describes the typical contents of certificate extensions and the qualifier types defined for the MegaSign CPS certificate policy identifier.

Name/Cert. Extension Fields	Purpose & Description	Accompanying English (or other human-readable) Text
General Extensions for CA and Subordinate CA:		
----------		
basicConstraints	*See* CPS § 7.1.2 (d)	Non Critical cA = TRUE
keyUsage	*See* CPS § 7.1.2 (e)	Non Critical KeyCertSign (Bit 5 set) CRLSign (Bit 6 set)
General Extensions for End-User Subscriber:		
----------		
basicConstraints	*See* CPS § 7.1.2 (d) *See* CPS § 7.1.2 (f)	Non Critical cA = FALSE
certificatePolicy		Non Critical *See* CPS § 7.1.2.7.3

MegaSign standard qualifier –Practices Reference	Contains text referring to the MegaSign repository (and in future versions of this CPS, certain non-MegaSign repositories), which holds the MegaSign CPS, CRL, and other information.	"**This certificate incorporates by reference, and its use is strictly subject to, the MegaSign Certification Practice Statement (CPS), available in the MegaSign repository at: https://www.megasign.nl; by E-mail at CPS-requests@megasign.nl; or by mail at Roccade Megaplex BV, Fauststraat 1, 7323 BA, Apeldoorn, The Netherlands Copyright (c)1999 Roccade Megaplex BV. Incorp. by Ref.,LIAB.LTD. (All Rights Reserved. Certain Warranties Disclaimed And Liability Limited.**"
MegaSign standard qualifier –cpsURLs	A single uniform resource locator indicating the source of this CPS.	**"https://www.megasign.nl/repository/CPS"**
MegaSign standard qualifier –NoticeID	An object identifier referring to a registered string whose content indicates information about warnings, cautions, warranty disclaimers, and limitations of liability regarding the use of MCS certificates. It is intended to be displayed with every certificate within the user agent (*e.g.,* computer or terminal) certificate viewing function (but it is not embedded in any certificate).	Registered string of value "**WARNING: USE OF THIS CERTIFICATE IS STRICTLY SUBJECT TO THE MEGASIGN CERTIFICATION PRACTICE STATEMENT. THE ISSUING AUTHORITY DISCLAIMS CERTAIN IMPLIED AND EXPRESS WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND, WILL NOT BE LIABLE FOR CONSEQUENTIAL, PUNITIVE, AND CERTAIN OTHER DAMAGES. SEE THE CPS FOR DETAILS.**"

MegaSign standard qualifier –NSINotice	An object identifier referring to a registered string whose content indicates that the certificate contains data for which the IA provides no assurances of accuracy.	Registered string of value "**Contents of the MegaSign registered nonverifiedSubjectAttribute extension value shall not be considered as information confirmed by the IA.**"

Table 14 – MegaSign Certificate Extensions

Alternatively a certificate contains, in a User Notice certificate policy qualifier, a reference to the following text which is displayed by certain products:

This certificate incorporates the MegaSign Certification Practice Statement (CPS) by reference. Use of this certificate is governed by the CPS.

The CPS is available in the MegaSign repository at :

http:/www.megasign.nl/repository; by E-mail at CPS-requests@megasign.nl; and by mail at Roccade Megaplex BV, Fauststraat 1, 7323 BA, Apeldoorn, The Netherlands, Attn: Certification Services.

> **THE CPS DISCLAIMS AND LIMITS CERTAIN LIABILITIES, INCLUDING CONSEQUENTIAL AND PUNITIVE DAMAGES. THE CPS ALSO INCLUDES CAPS ON LIABILITY RELATED TO THIS CERTIFICATE. SEE THE CPS FOR DETAILS.**

The CPS and this certificate are copyrighted: Copyright (c) 1999 Roccade Megaplex BV. All Rights Reserved

7.1.3 Algorithm object identifiers

Currently not used.

7.1.4 Name forms

a) Generally

See CPS §§ 3.1(b), 3.1.1-3.1.6.

b) Enhanced Naming

All end-user subscriber certificates, except for certain S/MIME v1 certificates, contain an additional "Organizational Unit" field — an X.520 attribute — that contains a brief statement regarding liability and incorporates by reference the complete CPS, such as "**OU= www.megasign.nl/repository/CPS (c) 1999** " (this references the primary URL of the CPS, notes that liability is limited, and includes a copyright notice). This or comparable information may be present in application-defined X.509 v3 extensions for display to users by "local" (non-MegaSign vendor controlled) means. Note: the content of this Organizational Unit field is abbreviated because of the X.509 limitation of 64 bytes. This usage of an Organizational Unit field will be retired when functional and consistent use of X.509 v3 extensions become ubiquitous.

See also item g of section 7.1.2 of this CPS.

7.1.5 Name constraints

All certificates issued as a result of a non-MegaSign organizational LRA's approval of a certificate application shall contain a distinguished name that states the affiliation of its subject.

7.1.6 Certificate policy Object Identifier

See CPS §§ 7.1.2 (f) -7.1.2 (g).

7.1.7 Usage of Policy Constraints extension

To Be Determined.

7.1.8 Policy qualifiers syntax and semantics

To Be Determined.

7.1.9 Processing semantics for the critical certificate policy extension

To Be Determined.

7.2 CRL Profile

7.2.1 Version number(s)

Currently CRL version 2 CRL's are used.

7.2.2 CRL and CRL entry extensions

Currently not used.

8 Specification administration

8.1 Specification change procedures

a) Amendments Generally

MegaSign shall be entitled to amend this CPS from time to time (prospectively and not retroactively). MegaSign shall be entitled to place amendments in the MegaSign repository either in the form of an amended version of the CPS or in the Practices Updates and Notices section of the MegaSign repository.

b) Practices Updates and Notices

Amendments to this CPS that are placed in the Practices Updates and Notices section of the MegaSign repository (*see* **https://www.MegaSign.nl/repository/updates**) shall have the effect of amending the CPS. Such amendments shall supersede any conflicting and designated provision(s) of the referenced version of the CPS.

c) Items That Can Change Without Notification

(c1) Non-Material Amendments

An amendment to the CPS that is non-material shall become effective immediately upon publication in the MegaSign repository in accordance with section 8.1 (a) of this CPS. MegaSign's decision to designate an amendment as non-material shall be within MegaSign's sole discretion.

(c2) Material Amendments Exception to CPS section 8.1.2

If, notwithstanding section 8.1.2, MegaSign publishes a material amendment to the CPS, it shall become effective immediately upon publication in the MegaSign repository in accordance with section 8.1(a) if failure by MegaSign to make the amendment may result in a compromise of the MCS or any portion of it.

d) Changes with Notification

A material amendment to the CPS shall become effective fifteen (15) days after MegaSign publishes the amendment in the MegaSign repository in accordance with section 8.1(a), unless MegaSign publishes a notice of withdrawal of the amendment in the repository prior to the end of such fifteen (15) day period.

e) Assent to Amendments

A certificate applicant and subscriber's decision not to request revocation of his, her, or its certificate within fifteen (15) days following the publication of an amendment shall constitute agreement to the amendment. See the MegaSign repository's "Practices Updates and Notices" section at **https://www.MegaSign.nl/repository/updates**.

Changes that will affect the associated trust-level will be addressed in a new version of the CPS. This must be approved by the CPS-board. All affected certificate users must obtain a new certificate.

8.2 Publication and notification policies

- Items not published in the CPS:
  - Comprehensive pricelist (available on request and under NDA*)
  - The MegaSign Security Procedures (available on request and under NDA*)
  - Ancillary agreements on the CPS (available on request and under NDA*).
- Distribution of CPS and CP's:

- The CPS and CP's are published on www.megasign.nl\repository
- The CPS and CP's are available on paper on request (at reasonable costs)

*please place request at MegaSign customer service desk or via E-mail: cps-request@megasign.nl

8.3 CPS approval procedures

Major changes in the MegaSign CPS and related CP's must be approved by the MegaSign CPS-Board.