



PKI Disclosure Statement Carl Zeiss AG – Email CA

Downloads, printed copies and copies of any kind of this document are not covered by the updating service!

Summary

This PKI disclosure statement is intended for the documentation of Email PKI with external communication partners. It describes the obligations of the subscriber and the external communication partner and how liability is regulated in the event of damage or loss.

Contents

1	Contact for certification centers	1
2	Type of certificate, validation procedures and use	1
3	Limitation of the use of the reliability of certificates (Reliance limits)	2
4	Obligations for subscribers.....	2
5	Obligations of the relying parties for the verification of the certificate status	2
6	Exclusion and liability limitation clauses....	2
7	Applicable agreements, certification practice statement, certificate policy	2
8	Data protection directives.....	2
9	Reimbursement directives.....	2
10	Governing Law and settlement of disputes clauses.....	2
11	CA and certificate directory licenses, confidentiality trademarks and audit.....	3
12	Abbreviations and Terms.....	3
13	Information on the document.....	3

1 Contact for certification centers

HP-CSD
Hewlett-Packard GmbH,
Carl-Zeiss-Strasse 22
73447 Oberkochen
Germany
Tel. +49 (0) 7364/ 20-6565
Fax +49 (0) 7364/ 954-280
Email: hp@zeiss.de

2 Type of certificate, validation procedures and use

In addition to the X.509 hierarchical infrastructure, the use of PGP with its “web of trust” model, in which keys and certificates are preferably used in accordance with X.509, is also supported. All statements in this PKI disclosure statement are based on both the hierarchical certification infrastructure in accordance with X.509 and the PGP, unless otherwise noted.

The Carl Zeiss AG email CA only issues certificates for users; no machine certificates are issued. The certificates must only be used for business purposes and for the following application:

- Email signature and encryption

Private use is not permitted.

The Carl Zeiss AG email CA validation procedure for the verification of the identity of the user certificates requires the user to have an email account at Carl Zeiss AG. For this, registration is based on the registration process and the verification of the identity which is performed by the Human Resources Department at Carl Zeiss AG when an employee is hired.

Private user keys are stored centrally on a secure email gateway and are protected against theft and unauthorized access.

The issuance of the Carl Zeiss AG email CA certificate is the responsibility of the Carl Zeiss AG Root CA administrators who are only allowed to operate under the four-eye principle. The Carl Zeiss AG Root CA validation procedure for verification of the identity of the Carl Zeiss AG email CA requires the following course of action:

1. Contacts for the email CA must be specified in writing in a document.
2. Certificate requests can be submitted personally on a data carrier or via email.
3. If this is done in person, issuance and return of the certificate occurs in a single process. The transfer is documented in writing.
4. In the email procedure, the email must generally have a digital signature and can be optionally encrypted. The application and transfer process shall be traceably documented.

The Carl Zeiss AG email CA certificate may only be used to issue email certificates for users.

3 Limitation of the use of the reliability of certificates (Reliance limits)

In accordance with the stated exclusion and liability limitation clauses (*limitation of liability*), email certificates from Carl Zeiss AG may only be used for authentication, integrity and confidentiality in the transmission of emails.

Liability is based on the generally applicable liability regulations within the scope of the respective application as they arise based on legislation and/or applicable agreements of the relying party with Carl Zeiss AG.

4 Obligations for subscribers

If a compromise is suspected, the subscriber must immediately inform the Carl Zeiss AG email CA and have the certificate cancelled. In other cases, the specifications in Chapter 6 apply.

5 Obligations of the relying parties for the verification of the certificate status

Before relying parties are allowed to trust an electronic signature, use a public key for encryption or accept the certificate for authentication¹, they must verify if the corresponding owner certificate is expired or has been revoked at the time of signature generation, encryption or authentication. Furthermore, they must ensure that the certification is suitable for the intended purpose.

The restricted lists used by Carl Zeiss AG PKI for X.509 certificates are published externally via HTTP.

6 Exclusion and liability limitation clauses

Unless otherwise explicitly regulated in an applicable agreement with a relying party and/or a subscriber, liability for material defects and defects of title and all liability of Carl Zeiss AG CA(s) regarding the creation, use, validity, suitability or correctness of certificates, including the identity of a person stated in a certificate or their authority to represent a company within the Carl Zeiss Group, is excluded except in cases of intent or gross negligence.

7 Applicable agreements, certification practice statement, certificate policy

The creation and application of Carl Zeiss AG certificates is based on the certification directives of the Carl Zeiss AG email CA.

The basis for the application of Carl Zeiss AG certificates by subscribers and relying parties is the present PKI disclosure statement alone.

8 Data protection directives

The obligation to data protection, which every Carl Zeiss AG employee must sign, is also valid when applying for certificates.

9 Reimbursement directives

Not applicable.

10 Governing Law and settlement of disputes clauses

The contract shall be governed by German law. The place of jurisdiction for all disputes shall be, at our discretion, our domicile or the domicile of the relying party; for lawsuits of the relying party jurisdiction shall be solely the domicile of the company of the Carl Zeiss Group that uses these conditions. Any statutory regulations governing exclusive

¹ Verification of the certificate for authentication is only relevant if a web mailer is used, which requires an SSL server certificate.

jurisdictional responsibilities shall remain unaffected.

11 CA and certificate directory licenses, confidentiality trademarks and audit

The Carl Zeiss AG PKI is subject to the general version of the Carl Zeiss AG.

12 Abbreviations and Terms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
HTTP	Hypertext Transfer Protocol
PDS	PKI Disclosure Statement

13 Information on the document

Change record

Version	Valid from	Change and reason	Preparation and checking
1.0	01.10.2006	First issue	Thomas Prim

Responsible for content	Author:
Thomas Prim Carl Zeiss AG Corporate Information Technology D-73446 Oberkochen Germany Tel: +49 (0) 7364/ 20-4575 Fax: +49 (0) 7364/ 854 111 prim@zeiss.de	Petra Barzin Secorvo Security Consulting GmbH D-76137 Karlsruhe Germany Tel.: +49 (0) 721/ 255171-0 Fax.: +49 (0) 721/ 255171-100 info@secorvo.de www.secorvo.de

Distribution

Published on the Carl Zeiss AG website
<http://www.zeiss.com/cert>

PGP **Pretty Good Privacy**

PKI **Public Key Infrastructure**

Subscribers

In general, subscribers are natural persons employed by Carl Zeiss AG. Additionally, the Carl Zeiss AG operating CA issues server certificates.

Relying Parties

Relying parties verify the authenticity of a subscriber based on a certificate from the Carl Zeiss operating CA. A relying party can also be a subscriber.