



PKI Disclosure Statement Carl Zeiss AG – E-Mail-CA

Downloads, Ausdrücke und Kopien jeglicher Art unterliegen nicht dem Änderungsdienst.

Zusammenfassung

Dieses PKI Disclosure Statement dient zur Dokumentation der E-Mail-PKI im Außenverhältnis mit externen Kommunikationspartnern. Es beschreibt, welchen Verpflichtungen die Zertifikatsinhaber und die externen Kommunikationspartner nachkommen müssen und wie die Haftung im Schadensfall geregelt ist.

Inhaltsverzeichnis

| | | |
|-----------|--|----------|
| 1 | Kontakt für Zertifizierungsstellen | 1 |
| 2 | Zertifikatstyp, Validierungsprozeduren und Verwendung | 1 |
| 3 | Begrenzung der Nutzung und der Verlässlichkeit von Zertifikaten (Reliance limits) | 2 |
| 4 | Verpflichtungen für Zertifikatsinhaber („Subscriber“)..... | 2 |
| 5 | Verpflichtungen der Relying Parties zur Zertifikatsstatusüberprüfung | 2 |
| 6 | Ausschluss- und Haftungsbegrenzungsklauseln | 2 |
| 7 | Anwendbare Vereinbarungen, Certification Practice Statement, Certificate Policy | 2 |
| 8 | Datenschutz-Richtlinien..... | 2 |
| 9 | Rückerstattungs-Richtlinien | 2 |
| 10 | Anwendbares Recht und Streitbeilegungsklauseln | 3 |
| 11 | CA und Zertifikatsverzeichnis Lizenzen, Vertraulichkeits-Warenzeichen und Audit .. | 3 |
| 12 | Abkürzungen und Begriffe | 3 |
| 13 | Informationen zum Dokument..... | 3 |

1 Kontakt für Zertifizierungsstellen

HP-CSD
Hewlett-Packard GmbH,
Carl-Zeiss-Straße 22
73447 Oberkochen,
Tel. +49-7364-20-6565
Fax +49-7364-954 280
E-Mail: hp@zeiss.de

2 Zertifikatstyp, Validierungsprozeduren und Verwendung

Neben der hierarchischen X.509-Infrastruktur wird auch der Einsatz von PGP mit seinem Vertrauensmodell „Web-of-trust“ unterstützt, wobei bevorzugt Schlüssel und Zertifikate nach X.509 verwendet werden. Alle in diesem PKI Disclosure Statement getroffenen Aussagen beziehen sich, wenn nicht anders angegeben, sowohl auf hierarchische Zertifizierungs-Infrastrukturen nach X.509 als auch auf PGP.

Die Carl Zeiss AG E-Mail-CA gibt nur Zertifikate für Benutzer aus; es werden keine Maschinenzertifikate ausgestellt. Die Zertifikate dürfen nur zu Geschäftszwecken und für die folgende Anwendung eingesetzt werden:

- E-Mail Signatur und Verschlüsselung

Eine private Nutzung ist nicht gestattet.

Die Validierungsprozedur der Carl Zeiss AG E-Mail-CA zur Überprüfung der Identität für Benutzerzertifikate erfordert, dass der Benutzer ein E-Mail-Account bei der Carl Zeiss AG hat. Dabei stützt sich die Registrierung auf den Registrierungsvorgang und die Überprüfung der Identität, die bei der Einstellung eines Mitarbeiters von der Personalabteilung der Carl Zeiss AG durchgeführt wurden.

Die privaten Benutzerschlüssel liegen zentral auf einem Secure-E-Mail-Gateway und müssen vor Diebstahl und unautorisiertem Zugriff geschützt werden.

Die Ausstellung des Carl Zeiss AG E-Mail CA Zertifikats obliegt den Carl Zeiss AG Root-CA Administratoren, die nur im 4-Augen Prinzip tätig werden können. Die Validierungsprozedur der Carl Zeiss AG Root-CA zur Überprüfung der Identität der Carl Zeiss AG Betriebs-CA erfordert folgende Vorgehensweise:

1. Ansprechpartner für die Betriebs-CA müssen in einem Dokument schriftlich benannt werden.
2. Zertifikatsanträge können persönlich durch Zertifikatsübergabe oder per E-Mail übermittelt werden
3. Bei persönlicher Übergabe erfolgt die Ausstellung und Rückgabe des Zertifikats in einem Prozeß. Die Übergabe wird schriftlich dokumentiert.
4. Beim E-Mail-Verfahren muss grundsätzlich digital signiert und kann optional verschlüsselt werden. Der Beantragungs- und Übergabeprozess wird nachvollziehbar dokumentiert.

Das Zertifikat der Carl Zeiss AG E-Mail-CA darf nur zur Ausstellung von E-Mail-Zertifikaten für Benutzer verwendet werden.

3 Begrenzung der Nutzung und der Verlässlichkeit von Zertifikaten (Reliance limits)

Gemäß den unten genannten Ausschluss- und Haftungsbegrenzungsklauseln (*Limitation of Liability*), dürfen E-Mail-Zertifikate der Carl Zeiss AG nur zum Zwecke von Authentifizierung, Integrität und Geheimhaltung bei der Übertragung von E-Mails angewendet werden.

Die Haftung richtet sich nach den im Rahmen des jeweiligen Anwendungsfalls gültigen allgemeinen Haftungsregeln, wie sie sich aufgrund der Gesetzeslage und/oder anwendbarer Vereinbarungen der Relying Party mit der Carl Zeiss AG ergeben.

4 Verpflichtungen für Zertifikatsinhaber („Subscriber“)

Wenn der Verdacht auf Kompromittierung besteht, muss der Zertifikatsinhaber unverzüglich die Carl

Zeiss AG E-Mail-CA informieren und das Zertifikat widerrufen lassen. Ansonsten gelten die Angaben aus Kapitel 6.

5 Verpflichtungen der Relying Parties zur Zertifikatsstatusüberprüfung

Bevor eine Relying Party einer elektronischen Signatur vertrauen, den öffentlichen Schlüssel zur Verschlüsselung verwenden oder das Zertifikat zur Authentisierung¹ akzeptieren darf, muss sie sich davon überzeugen, dass das entsprechende Inhaber-Zertifikat zum Zeitpunkt der Signaturerstellung, der Verschlüsselung oder der Authentisierung weder zurückgezogen wurde noch abgelaufen ist. Weiterhin muss sie sich vergewissern, dass das Zertifikat für die beabsichtigten Zwecke geeignet ist.

Die von der Carl Zeiss AG PKI verwendeten Sperrlisten (CRLs) für X.509 Zertifikate werden extern über HTTP veröffentlicht.

6 Ausschluss- und Haftungsbegrenzungsklauseln

Wenn nicht ausdrücklich in einer anwendbaren Vereinbarung mit einer Relying Party und/oder einem Zertifikatsinhaber anders geregelt, ist eine Haftung für Sach- und Rechtsmängel und jegliche Haftung von Carl Zeiss AG CA(s) bezüglich der Erstellung, Nutzung, Gültigkeit, Eignung oder Richtigkeit von Zertifikaten einschließlich der in einem Zertifikat benannten Identität einer Person oder ihrer Autorität, eine Gesellschaft der Carl Zeiss Gruppe zu vertreten - außer bei Vorsatz oder grober Fahrlässigkeit - ausgeschlossen.

7 Anwendbare Vereinbarungen, Certification Practice Statement, Certificate Policy

Die Erstellung und Anwendung von Carl Zeiss AG Zertifikaten richtet sich nach der Zertifizierungsrichtlinie der Carl Zeiss AG E-Mail-CA.

Grundlage für die Anwendung von Carl Zeiss AG Zertifikaten durch Zertifikatsinhaber und Relying Parties ist alleine das vorliegende PKI Disclosure Statement.

8 Datenschutz-Richtlinien

Die Verpflichtung auf den Datenschutz, die jeder Mitarbeiter der Carl Zeiss AG unterschreiben muss, gilt auch für die Beantragung von Zertifikaten.

9 Rückerstattungs-Richtlinien

Nicht zutreffend.

¹ Die Überprüfung des Zertifikats zur Authentisierung ist nur bei Verwendung des Web-Mailers relevant, welcher ein SSL Server Zertifikat benötigt.

10 Anwendbares Recht und Streitbeilegungsklauseln

Es gilt deutsches Recht. Gerichtsstand für alle Streitigkeiten ist nach unserer Wahl unser Sitz oder der Sitz der Relying Party, für Klagen der Relying Party ausschließlich der Sitz des diese Bedingungen verwendenden Unternehmens der Carl Zeiss Gruppe. Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

11 CA und Zertifikatsverzeichnis Lizenzen, Vertraulichkeits-Warenzeichen und Audit

Die Carl Zeiss AG PKI unterliegt der allgemeinen Revision der Carl Zeiss AG.

12 Abkürzungen und Begriffe

| | |
|------------|---|
| CA | Certification Authority Zertifizierungsstelle |
| CP | Certificate Policy Zertifizierungsrichtlinie |
| CPS | Certification Practice Statement Regelungen für den Zertifizierungsbetrieb |
| CRL | Certificate Revocation List Sperrliste |

13 Informationen zum Dokument

Änderungsliste

| Version | Gültig ab | Änderung und Grund | Erstellung & Prüfung |
|---------|------------|--------------------|----------------------|
| 1.0 | 01.10.2006 | Erstausgabe | Thomas Prim |

| Verantwortlich für den Inhalt | Ersteller |
|---|---|
| Thomas Prim Carl Zeiss AG Konzernfunktion Informationstechnologie D-73446 Oberkochen Tel: +49 7364 20-4575 Fax: +49 7364 854 111 prim@zeiss.de | Petra Barzin Secorvo Security Consulting GmbH D-76137 Karlsruhe Tel.: +49 721 255171-0 Fax.: +49 721 255171-100 info@secorvo.de www.secorvo.de |

Verteilung

Veröffentlichung im Internetauftritt der Carl Zeiss AG
<http://www.zeiss.com/cert>

HTTP Hypertext Transfer Protocol

PDS PKI Disclosure Statement

PGP Pretty Good Privacy

PKI Public Key Infrastructure

Zertifikatsinhaber (Subscribers)

Zertifikatsinhaber sind in der Regel natürliche Personen, die bei der Carl Zeiss AG angestellt sind. Die Carl Zeiss AG Betriebs-CA stellt darüber hinaus auch Serverzertifikate aus.

Zertifikatsprüfer (Relying Parties)

Zertifikatsprüfer (Relying Parties) überprüfen anhand eines Zertifikates der Carl Zeiss AG Betriebs-CA die Authentizität eines Zertifikatsinhabers. Ein Zertifikatsprüfer kann gleichzeitig Zertifikatsinhaber sein.