Stadtwerke
Bochum | Netz

PKI Disclosure Statement der
Stadtwerke Bochum Netz GmbH E-Mail CA

Öffentliche Informationen zur E-Mail CA

Inhaltsverzeichnis

1 Kontakt der Zertifizierungsstelle

Adresse: rku.it
Westring 301
44629 Herne
Telefon: +49 2323 3688-0
Mail: it-sicherheit@rku-it.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 E-Mail CA stellt Zertifikate für Mitarbeiter oder ihre Kunden aus. Die Zertifikate dürfen nur zu Geschäftszwecken und ausschließlich für E-Mail Signatur und Verschlüsselung eingesetzt werden. Die private Nutzung der Schlüssel und Zertifikate ist analog zur Nutzung privater E-Mail im Unternehmen geregelt.
Schlüssel und Zertifikate für Benutzer und Funktionen werden bei Bedarf automatisch von der E-Mail CA ausgestellt, so dass kein Registrierungsprozess und keine explizite Validierungsprozedur erfolgt. Die Authentifizierung von Benutzern erfolgt auf Basis ihrer E-Mail Adressen, d.h. durch Zugriff und Versenden einer E-Mail von ihrem E-Mail Account.
Ebenso erfolgt die Authentifizierung von Funktionsträgern durch Zugriff und Versenden einer E-Mail von ihrem funktionsgebundenem E-Mail Account. Die Daten der Zertifikatsinhaber werden aus einem internen LDAP Verzeichnis bezogen. Die Identität eines Benutzers wird beim Einstellungsprozess überprüft, bevor ein neuer Benutzereintrag im internen Verzeichnis angelegt wird. Die privaten Benutzerschlüssel liegen zentral auf einem Secure E-Mail Gateway und werden dort zuverlässig vor Diebstahl und unautorisiertem Zugriff geschützt. Sowohl die E-Mail CA als auch die Benutzer verwenden Schlüssel mit einer Schlüssellänge von 2048 Bits.

3 Begrenzung der Nutzung und der Verlässlichkeit von Zertifikaten

Gemäß den unten genannten Ausschluss- und Haftungsbegrenzungsklauseln dürfen Zertifikate, die von der E-Mail CA ausgestellt wurden, nur zum Zwecke von Authentifizierung, Integrität und Geheimhaltung von E-Mails verwendet werden.
Eine spezielle Haftungsregelung für die E-Mail CA ist nicht vorgesehen; 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 rku.it GmbH ergeben.

4 Verpflichtungen für Zertifikatsinhaber

Wenn der Verdacht auf Kompromittierung besteht, muss der Zertifikatsinhaber unverzüglich die E-Mail CA informieren und das Zertifikat widerrufen lassen. Ansonsten gelten die Angaben aus Abschnitt 6.

5 Verpflichtungen der Relying Parties zur Zertifikatsstatusüberprüfung

Bevor eine Relying Party einer elektronischen Signatur vertrauen oder den öffentlichen Schlüssel zur Verschlüsselung verwenden darf, muss sie sich davon überzeugen, dass das zugehörige Zertifikat zum Zeitpunkt der Signaturerstellung oder Verschlüsselung weder zu-

rückgezogen wurde noch abgelaufen ist. Weiterhin muss sie sich vergewissern, dass das Zertifikat für die beabsichtigten Zwecke geeignet ist.
Die Sperrliste der E-Mail CA ist extern über HTTP und LDAP veröffentlicht. Der Verweis auf die Sperrliste ist in jedem ausgestellten Zertifikat enthalten.

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 der E-Mail CA bezüglich der Erstellung, Nutzung, Gültigkeit, Eignung oder Richtigkeit von Zertifikaten einschließlich der in einem Zertifikat benannten Identität einer Person oder Funktion - außer bei Vorsatz oder grober Fahrlässigkeit - ausgeschlossen.

7 Anwendbare Vereinbarungen, Certification Practice Statement, Certificate Policy

Die Erstellung und Verwaltung von Zertifikaten durch die E-Mail CA richtet sich nach den Regelungen zum Zertifizierungsbetrieb der E-Mail CA. Diese Regelungen sind in einem internen Dokument „Certification Practice Statement“ beschrieben. Auf Nachfrage kann Einsicht in diese Regelungen zum Zertifizierungsbetrieb gewährt werden.
Grundlage für die Anwendung von Zertifikaten durch Zertifikatsinhaber und Relying Parties ist alleine das vorliegende PKI Disclosure Statement.

8 Datenschutz-Richtlinien

Die CA-Administratoren der E-Mail CA sind zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet.

9 Rückerstattungs-Richtlinien

Nicht zutreffend.

10 Anwendbares Recht und Streitbeilegungsklauseln

Rechtliche Auseinandersetzungen, die aus dem Betrieb der E-Mail CA herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland. Erfüllungsort und ausschließlicher Gerichtsstand ist Sitz des IT-Dienstleisters rku.it.

11 CA und Zertifikatsverzeichnis Lizenzen, Vertraulichkeits-Warenzeichen und Audit

Der Betrieb der E-Mail CA unterliegt der allgemeinen Revision der rku.it GmbH und wird jährlich auditiert.