

c't Krypto-Kampagne Zertifizierungsantrag

Checkliste:

1. Schlüssellänge mindestens 1024 Bit (min. 768 Bit, falls vor 1.1.97 erzeugt)
2. jede zu zertifizierende Benutzerkennung muß ein Eigenzertifikat tragen
3. Formular bitte vollständig ausfüllen (Unterschrift nicht vergessen)
4. per E-Mail an pgpCA@ct.heise.de senden (oder Public-Keyblock auf beschrifteter Diskette abgeben)
5. mit einem gültigen Personalausweis/Reisepass den Heise-Stand besuchen

Persönliche Daten:

Name, Vorname: _____

Straße, Hausnr.: _____

PLZ, Ort: _____

ausgewiesen durch Personalausweis, Nummer: _____

geprüft:

PGP-Public-Key-Daten:

Benutzerkennung: _____

Key-ID: _____

vom (Datum): _____

Schlüsselart: RSA DSS/DH (DSA/El Gamal) Länge: _____ / _____ Bit

Fingerprint: _____ (hexadezimal)

Meinen PGP-Public-Key habe ich (bitte ankreuzen):

- mit _____ zusätzlichen Benutzerkennungen versehen
- auf _____ beigefügt (bitte beschriften - Rückversand ausgeschlossen)
- per E-Mail an pgpCA@ct.heise.de geschickt

Ich bitte um die Zertifizierung meines PGP-Schlüssels. Mit der Weitergabe des signierten Schlüssels an PGP-Keyserver bin ich einverstanden. Der signierte Schlüssel geht mir per E-Mail an die in der primären Benutzerkennung genannte Adresse zu.

Von folgenden Hinweisen habe ich Kenntnis genommen:

Die in den Schlüsseln enthaltenen E-Mail-Adressen werden mit veröffentlicht, und sind im weltweiten PGP-Keyserver-Verbund von jedermann einsehbar. Es ist nicht auszuschliessen, dass die PGP-Schlüssel und die enthaltenen Benutzer-IDs von E-Mail-Adress-Sammlern z.B. für Spamzwecke missbraucht werden. Eine Veröffentlichung ist nicht rückgängig zu machen.

Die Daten dieses Antrags werden ausschließlich zur Archivierung der Identitätsprüfung genutzt und weder zu Marketingzwecken verwendet noch an Dritte weitergegeben; eine elektronische Erfassung bleibt vorbehalten. Der Zertifizierung kommt keinerlei rechtliche Bedeutung zu. Es besteht kein Anspruch auf Erteilung eines Zertifikats.

Datum, Unterschrift _____, _____