if(is) Institut für Internet-Sicherheit – if(is), Neidenburger Str. 43, 45897 Gelsenkirchen

Zertifizierungsantrag

Persönliche Daten:

Name, Vorname:

Straße, Hausnr.:

PLZ, Ort:

Dokument: ◯ Personalausweis ◯ Reisepass Nummer:

– muss von der if(is)-ZI ausgefüllt werden –

☐ **Angaben zur Identität erfolgreich vom if(is) überprüft**

Datum, Unterschrift _____ , _____

Public-Key-Daten:

Benutzerkennung (E-Mail):

Key-ID:

vom (Datum):

Schlüsselart: ◯ RSA ◯ DSS/DH (DSA) Länge: / Bit

◯ Curve 25519 ◯ NIST P-512 ◯ Brainpool P-512 ◯ Sonstiges

Fingerprint (hexadezimal):

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

☐ mit einem Eigenzertifikat versehen (erforderlich!)

☐ mit zusätzlichen Benutzerkennungen versehen:

☐ per E-Mail an pgpZI@internet-sicherheit.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 nach der Bestätigung meiner E-Mail-Adresse(n) per E-Mail an die in der primären Benutzerkennung genannte E-Mail-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 sowie zur Verifizierung der E-Mail-Adresse(n) 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.

Von den vollständigen Richtlinien, die unter https://www.internet-sicherheit.de/pgpZI/policy zu finden sind, habe ich ebenfalls Kenntnis genommen.

Datum, Unterschrift _____ , _____