
Erklärungen zum Datenformat für CA-Lieferungen von PGP-Schlüsseln

V1.01

ORG:

Der Name der liefernden CA

Beispiel: CA Universitaet Tuebingen

SIG:

DATASET des Puplic-Keys der zertifizierenden CA, der zur Signatur verwendet wird.

Beispiel:
SIG001

FORMAT:

Versionsnummer des Format, das für diese Datenlieferung verwendet wurde.

Beispiel: 1.01

Schlüsselbegriff:

Schlüsselbegriffe sind Einträge im Datenlieferungsformular, die sowohl der Gliederung des Formulars, als auch der Steuerung der Datenverarbeitung dienen. Sie sind obligatorisch und müssen angegeben werden.

DATASET:

ID des PGP-Schlüssel-Datensatzes. Diese ID wird von der zertifizierenden CA vergeben und dient der eindeutigen identifizierung des PGP-Schlüssels.

Beispiel: 19990314009

ACTION:

Gibt an wie mit dem Datensatz verfahren werden soll

new-dataset

Ein Datensatz soll neu angelegt werden.

revoke-key

Ein PGP-Schlüssel des Datensatzes soll revoked werden.

invalidate-key

Ein PGP-Schlüssel des Datensatzes soll für ungültig erklärt werden.

remove-dataset

Ein Datensatz soll aus dem Verzeichnis entfernt werden.

remove-all

Alle von der CA zertifizierten PGP-Schlüssel sollen aus Verzeichnis entfernt werden.

REVOKER:

Wer veranlasst die Revokation eines PGP-Schlüssels

USER

Der Benutzer selbst widerruft seinen Schlüssel.

CA

Die CA widerruft einen (Benutzer)-Schlüssel.

USER

DN (Distinquished Name) des Benutzers im X500

Beispiel: cn=Lieschen Mueller,ou=Studierende,ou=Medienforschung,o=UniversitaetTuebingen,l=DFN,c=DE

LABEL

Text für die Bezeichnung des Links auf den Keyserver

new `TEXT`

Key wird neu eingetragen.

keep

Key wird zurückgezogen, der Link auf den zurückgezogenen Key soll aber weiterhin bestehen bleiben.

delete

Key wird zurückgezogen, der Link auf den zurückgezogenen Key soll gelöscht werden.

Key:

Der öffentliche PGP-Key des Benutzers in ASCII-Armored Form (base64 encoded).

Beispiel:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzZmgLsAAAEEAJq/xL+nvPHYnt+qPWbRK+Y44DayVBmTJKNaqnXOu3KlY3TR
AU/8YJ4pv2KlFGYdsMGKM0MnEjfVPRvcB2qJjDyq9UFD4YUsB2aQsD3hVueHN0sC
s3L3yB6nJrBBy8+EJFwghbMOZL7Zy2yVNc3/b6YVhB+NRXnoiII9p9H+8zqVAAUR
tDBNYXJrdXMgU2F1ZXIgPG1hcmt1cy5zYXVlckB6ZHYudW5pLXR1ZWJpbmdlbi5k
ZT6JAJUDBRA2ZoNf1sNKtX1rroUBAdb4A/wJYNw5l1WP74DsO5CtTuB2cy41DqEo
iZCre4omN6mcMOwWerQeAQ36eO8zeD5S89OwF9yRwHat83b0fO1q0PxXb9+H2V1j
bMSKB5wq0VhmJNp0qlY/FkpbH3vy6JeH1PjobbMxbuHFCBOMUjA2tlYpzlg8spR3
BvmSX+BCyYYd4IkAlQMFEDZmgLuCPafR/vM6lQEBozQD/0fDZljdStGoBSXSCj56
xalMRgs0isWEayiRAtMnScZwVeNiuacF4AL3v0Ix5Hn8k9yfcc/Mmkwh5KqsGX2O
yb01bR7Qd+7vpZy/W88NvErTR0yHBAKLAyjwxePanE29/u90h854Xz54FK+CsNeD
iqQmPGpig3P8i2sA6VZw4R+0tAZNYXJrdXM=
=Q1dX
-----END PGP PUBLIC KEY BLOCK-----
```


END-OF-KEY

Key-ID:

KEY-ID des PGP-Keys des Benutzers.

Beispiel: DEC33A82

USER-ID

User IDs des PGP-Schlüssel des Benutzers

Beispiel: `Hans Mustermann hans.mustermann@xyz.abc.de`

PRIME-USER-ID

Primäre User ID des PGP-Schlüssel des Benutzers.

Beispiel: `Hans Mustermann hans.mustermann@xyz.abc.de`

FINGERPRINT:

FINGERPRINT des PGP-Keys des Benutzers

Beispiel: `44 F6 00 1C F2 39 B8 1A AA 62 18 0A C6 93 0F CF`

KEYSIZE:

Länge des des PGP-Keys des Benutzers in Bit. Immer in fuenfstellig angeben.

Beispiel: 01024

KEYTYPE

Algorithmen, die zur Generierung des Keys und des Hash benutzt wurden.

key-algo.

DSS/DH

hash-algo.

SHA1

PGPVERSION:

Version der PGP-Software, die zur Generierung des Schlüssels eingesetzt wurde

---

CREATION:

Datum des Tages an dem der PGP-Schlüssel erzeugt wurde.
Das Format ist dabei Jahr-Monat-Tag.

Beispiel: 1999-02-23

EXPERATION:

Datum des Tages an dem der PGP-Schlüssel seine Güsltigkeit verlieren soll.
Das Format ist dabei Jahr-Monat-Tag.

Beispiel: 2001-04-01

USAGE

Verwendungszeck des PGP-Schlüssels

CN:

Voller Name des Benutzer

Beispiel: Karl Heinz Mustermann

SN:

Nachname des Benutzers

Beispiel: Mustermann

MAIL:

Mailadresse des Benutzers

Beispiel: karl-heinz.mustermann@abc.xyz.de

DESCRIPTION:

Beschreibung des Schlüssels / Benutzers

Beispiel: Karl-Hans Mustermann, Zimmer C4711, Bibliothekar

KEYOWNER

Welchen Status hat der Besitzer des Schlüssels

USER

Der Besitzer des Schlüssels ist normaler Benutzer

CA

Bei dem Schlüssel handelt es sich um einen CA-Schlüssel

RA

Bei dem Schlüssel handelt es sich um einen RA-Schlüssel

CREATIONMODE:

Wie / von wem wurde der Schlüssels generiert

USER

Der Schlüssel wurde vom Benutzer selbst erzeugt

CA

Der Schlüssel wurde von einer Application automatisch erzeugt

CA

Der Schlüssel wurde von der zertifizierenden CA erzeugt

RA

Über die Generierung des Schlüssels gibt es keine Informationen

---

CA-POLICY:

Link auf die Policy der zertifizierenden CA

Beispiel: http://www.pca.dfn.de/dfnpca/policy/wwwpolicy.html

CA-DN:

CN der zertifizierenden CA

Beispiel: cn=pca,o=dfnpca,l=dfn,c=de
cn=Lieschen Mueller,ou=Instiut fuer Tierkrankheiten,o=Universitaet Tuebingen,l=DFN,c=DE

CA-CRLLINK:

Link auf die CRL der zertifizierenden CA

Beispiel: http://www.pca.dfn.de/dfnpca/certify/ssl/pca-crl.html

---

REVCERT

Wurde ein Revokation-Zertifikat bei der zertifizierenden CA hinterlegt?

YES

Revokation-Zertifikat wurde hinterlegt

NO

Revokation-Zertifikat wurde nicht hinterlegt
