Beschreibung des Datenformats v1.01 für die Übermittlung von PGP-Schlüsseldaten durch eine CA

Stand: 30. Juli 1999

Kontakt:

DFN Directory Services Deutschland
Zentrum für Datenverarbeitung Universität Tübingen
Wächterstr. 76
D-72074 Tübingen
Tel. +49 7071 2970335 / +49 7071 2970336 / +49 7071 2970334
Fax. +49 7071 295912
E-Mail: dirco-ca-support@directory.dfn.de

0. Einleitung

Im folgenden wird beschrieben, wie dem Projekt DFN-DSD PGP-Schlüsseldaten durch die zertifizierenden CAs übermittelt werden koennen. Das zur Übermittlung verwendete Datenformat wird allgemein und anhand von Fallbeispielen beschrieben.

Folgende Aktionen auf dem DSD PGP-Keyserver sind über das Datenformat möglich:

-- Neueintrag von Schlüssel
-- Revokation von Schlüssel
-- ungültig Markieren von Schlüssel
-- Entfernen von Schlüssel
-- Entfernen aller Schlüssel, die durch eine CA zertifiziert wurden

Es werden folgende Versionen von PGP unterstützt: 2.6.x, 5.x, 6.x

1. Übermittlung der Daten

PGP-Schlüsseldaten werden per anonymous FTP auf den Rechner

ftp-ambix.directory.dfn.de

übertragen.

Die Dateien müssen von den CAs mit deren Signaturschlüssel signiert und mit dem PGP Schlüssel von

DDSD PGP-Keyserver Carrier <dirco-pgp@directory.dfn.de>

verschlüsselt werden.

Auf diesem Rechner ist ein Unterverzeichnis 'incoming' angelegt, in das die Daten abgelegt werden. Der FTP-Server ist so konfiguriert, dass der Schutz der Daten sichergestellt ist. Daten einer CA werden unter dem Namen

< ca-name > .pgp

abgelegt. Was anstelle von < ca-name > jeweils anzugeben ist, wird bei der Kontaktaufnahme mit der CA vereinbart
Beispiele fuer gueltige Namen sind:

ca-tue.pgp
ca-hh.pgp

Nach erfolgter Datenübertragung ist dem Projekt unter der Mail-Adresse

dirco-ca-pgp@directory.dfn.de

eine entsprechende Benachrichtigung zuzustellen, in welcher der zur Datenablage benutzte Dateinamen genannt wird.

2. Datenformat für die Bereitstellung von PGP-Schlüsseldaten

Eine komplette Definition des PGP-Schlüssel-Datensatzes mit Erläuterungen und Beispielen findet sich hier.

2.1 Header und Datenblock

Im Datenfile müssen vor den eigentlichen PGP-Schlüsseldaten in einem Header-Bereich Angaben zur CA und dem verwendeten Signaturschlüssel enthalten sein. Die Information über den Signaturschlüssel wird zum Aufbau einer 'Chain of Trust' durch die Zertifizierungshierachie verwendet.

Die Schlüsselworte zu Beginn der Zeilen sind in der hier angegebenen Schreibweise zu benutzen, der Doppelpunkt als Abschluß des Schlüsselworts ist obligatorisch.

Der eigendliche Datenblock wird von dem Steuerbegriff 'DATA' markiert Jeder Datensatz für einen PGP-Schlüssel befindet sich in einem Block, dessen Begin mit dem Steuerbegriff 'BEGIN-OF-KEYDEF' und dessen ENDE mit dem Steuerbegriff 'END-OF-KEYDEF' markiert wird. Bitte beachten Sie, daß bei diesen drei Steuerbegriffen kein abschliessender Doppelpunkt folgen darf.

Der Datenblock darf dabei beliebig viele Datensätze enthalten. Zu beachten ist dabei lediglich, daß alle Schlüssel mit dem selben Signaturkey signiert sein müssen, da dieser bereits im HEADER vereinbart wird.

Das Datenfile erhält damit folgende Struktur:

ORG:	`Name der CA`
SIG:	`Dataset des CA-Signatur-Schlüssels`
FORMAT:	`Version der Datendefiniton`

DATA

BEGIN-OF-KEYDEF

Datensatz des 1. PGP-Schlüssels

END-OF-KEYDEF

BEGIN-OF-KEYDEF

Datensatz des 2. PGP-Schlüssels

END-OF-KEYDEF

. . . . .

BEGIN-OF-KEYDEF

Datensatz des n. PGP-Schlüssels

END-OF-KEYDEF

2.2 Struktur eines PGP-Schlüssel Datensatzes

Nachfolgend wird die Struktur eines Datensatzes dargestellt. Der Anfang jedes Datensatzes wird durch den Schlüsselbegriff ’BEGIN-OF-KEYDEF’, sein Ende durch den Schlüsselbegriff ’END-OF-KEYDEF’ markiert.

Die Reihenfolge der Schlüsselworte ist unerheblich. Kommentare werden durch ein ’#’ zu Beginn der Zeile markiert. Leerzeilen werden ignoriert.

Die Schlüsselworte zu Beginn der Zeilen sind in der hier angegebenen Schreibweise zu benutzen, der Doppelpunkt als Abschluß des Schlüsselworts ist obligatorisch.

Unter ’Inhalt’ werden in der nachfolgenden Tabelle, sofern bestehend, alle bestehenden Möglichkeiten aufgeführt. Einige Angaben sind optional, diese sind mit einem ’x’ gekennzeichnet.

Schlüsselwort	**Inhalt**
BEGIN-OF-KEYDEF	
DATASET:	`ID des Datensatzes`
ACTION:	`(new-dataset/revoke-dataset/invalidate-key/remove-dataset/remove-`
KEY:	`ASCII Armored Key`
END-OF-KEY	`Schlüsselbegriff`

LABEL:	(new TEXT/keep/delete)
USER:	X.500-DN des Benutzers
CN:	Name des Benutzers
SN:	Nachname des Benutzers
MAIL:	Mailadresse(n)
DESCRIPTION:	Beschreibung
KEYOWNER:	(USER/CA/RA)
CREATIONMODE:	(OWN/AUTO/CA/UNKNOWN)
REVCERT:	(YES/NO)
REVOKER:	(USER/CA)

END-OF-KEYDEF

3 Beispiele für Datenlieferungen

Im nachfolgenden Abschnitt werden Beispiele für die möglichen Aktionen auf dem DSD PGP-Keyserver gegeben.

3.1 Neueintrag eines Schlüssels

Datenlieferung durch die CA Universitaet Tuebingen
vom 18. Juli 1999

ORG:	CA Universitaet Tuebingen
SIG:	sig001
FORMAT:	1.01

DATA

BEGIN-OF-KEYDEF

DATASET:	user-19990612-007
ACTION:	new-dataset

KEY:

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

mQCNAzdlCAgAAAEEAJ2W+ZHzVk+UThtAkxOcEhPPPERF71pJEzixNPyFK55GWxdT
5a0/RAKkEDeCgejc5tuz+fHqF+X7vzwz88s4gtkjWj+YTMOqHOKfLAH0iQmAXVTD
KeCsYxV5TK4mQOz/y3ks3jFYt+2pg+HyDuNpLkBvrkrweeFRNcKm2VY/8ydFAAUR
tCxNYXJrdXMgU2F1ZXIgPE1hcmt1cy5TYXVlckBkaXJlY3RvcnkuZGZuLmRlPokA
```

lQMFEDdlAdb28v6AvoKyTQEBFRgEALsWMF+QHblwjhYlGf8F5iANBWPKtS8or2+C
+x6bm6pOxFCwGDruN/VwXm7BbzN4oqJxfi8xDWAa29T7MgdymseAJklNs7X3esr0
Wu9+yBzmG6Nzwv5Uk8Q4cszW5/Xy26CqGjWZzkUVZpaPXqVvX2Y092Xm+4g6EeVA
pv5gadjIiQCVAwUQN2UICMKm2VY/8ydFAQHDKAP6AqGwSGqOMh62+lLr+2lNP5mf
9iI0CQfyWoX85AZHp7bY7n5wAUEY0yZY9IwOFAAqbtVgtDo1gIvacZ495xPM6wsS
/TSrJ0hLC3TU6R3ro9X8tUxnC5dty5xv4+LtWchQbfXHl6ANWh+FKzWMEwy18o29
7u3EeUciblyKIdBmqtQ=
=vM3u
-----END PGP PUBLIC KEY BLOCK-----

END-OF-KEY

KEYOWNER: USER

CREATIONMODE: OWN

optionale Angaben

LABEL: new PGP-Key fuer private Mails

USER: cn=Hans Mustermann,o=AMBIX,l=DFN,c=DE

CN: Hans Mustermann

SN: Mustermann

MAIL: hans.mustermann@directory.dfn.de

DESCRIPTION: PGP Schlüssel zur Signatur und Verschlüsselung priv. Mails

REVCERT: YES

END-OF-KEYDEF

3.2 Revokation eines Schlüssels

Datenlieferung durch die CA Universitaet Tuebingen
vom 18. Juli 1999

ORG: CA Universitaet Tuebingen

FORMAT: 1.01

DATA

BEGIN-OF-KEYDEF

DATASET: user-19990612-007

ACTION: revoke-key

KEY:

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

mQCNAzdlCAgAAAEEAJ2W+ZHzVk+UThtAkxOcEhPPPERF71pJEzixNPyFK55GWxdT
5a0/RAKkEDeCgejc5tuz+fHqF+X7vzwz88s4gtkjWj+YTMOqHOKfLAH0iQmAXVTD
KeCsYxV5TK4mQOz/y3ks3jFYt+2pg+HyDuNpLkBvrkrweeFRNcKm2VY/8ydFAAUR
tCxNYXJrdXMgU2F1ZXIgPE1hcmt1cy5TYXVlckBkaXJlY3RvcnkuZGZuLmRlPokA
lQMFEDdlAdb28v6AvoKyTQEBFRgEALsWMF+QHblwjhYlGf8F5iANBWPKtS8or2+C
+x6bm6pOxFCwGDruN/VwXm7BbzN4oqJxfi8xDWAa29T7MgdymseAJklNs7X3esr0
Wu9+yBzmG6Nzwv5Uk8Q4cszW5/Xy26CqGjWZzkUVZpaPXqVvX2Y092Xm+4g6EeVA
pv5gadjIiQCVAwUQN2UICMKm2VY/8ydFAQHDKAP6AqGwSGqOMh62+lLr+2lNP5mf
9iI0CQfyWoX85AZHp7bY7n5wAUEY0yZY9IwOFAAqbtVgtDo1gIvacZ495xPM6wsS
/TSrJ0hLC3TU6R3ro9X8tUxnC5dty5xv4+LtWchQbfXHl6ANWh+FKzWMEwy18o29
7u3EeUciblyKIdBmqtQ=
=vM3u
-----END PGP PUBLIC KEY BLOCK-----

END-OF-KEY

LABEL: keep

REVOKER: USER

END-OF-KEYDEF

3.3 Entfernen eines Schlüssels

\# Datenlieferung durch die CA Universitaet Tuebingen
\# vom 18. Juli 1999

ORG: CA Universitaet Tuebingen

FORMAT: 1.01

DATA

BEGIN-OF-KEYDEF

DATASET: user-19990612-007

ACTION: remove-dataset

END-OF-KEYDEF

3.4 Entfernen aller Schlüssel, die von einer CA zertifiziert wurden

\# Datenlieferung durch die CA Universitaet Tuebingen
\# vom 18. Juli 1999

ORG: CA Universitaet Tuebingen
FORMAT: 1.01

DATA

BEGIN-OF-KEYDEF
ACTION: remove-all
END-OF-KEYDEF

3.4 Ungültig Markieren eines Schlüssels

Datenlieferung durch die CA Universitaet Tuebingen
vom 18. Juli 1999

ORG: CA Universitaet Tuebingen
FORMAT: 1.01

DATA

BEGIN-OF-KEYDEF
DATASET: user-19990612-007
ACTION: invalidate-key
LABEL: keep
END-OF-KEYDEF