Datenformat für CA-Lieferungen von PGP-Schlüsseln V1.01

Momentan werden folgende Versionen von PGP unterstützt: PGPv2, PGPv5.

H E A D E R		
Keyword	**Inhalt**	**opt.**
ORG:	< Name der Organisation >	
SIG:	< DATASET des CA-SIGNATUR-Schlüssels >	
FORMAT:	< Version der Datendefiniton >	
DATA:	Schlüsselbegriff markiert Beginn gelieferten PGP-Daten	

D A T E N S A T Z					
		Modus			
Keyword	**Inhalt**	**new**	**rev**	**Kommentar**	**op**
BEGIN-OF-KEYDEF		x	x	Schlüsselbegriff markiert den Begin des Datensatzes eines Users	
DATASET:	< ID des Datensatzes >	x	x	Vorgabe durch CA	

ACTION:	new-dataset	x		Key neu eintragen	
	revoke-key		x	Key revoken	
	invalidate-key		x	Key ungültig markieren	
	remove-dataset			(User-)Key löschen	
	remove-all			nur CA: Alle UserKeys, die zertifiziert wurden löschen	
REVOKER:	User		x	Wer veranlasst die Revokation des/der Schlüssel	
	CA		x		
USER:	< DN des Users>	x		kann auch CA sein	x
LABEL:	new< ldapURL-Label>	x		Key wurde neu angelegt, Label für ldapURL auf PGP-Key im Usereintrag	x
	keep		x	Key wurde revoked, behalte Link auf revoked Key	x
	delete		x	Key wurde revoked, entferne Link auf revoked Key	x
KEY:	< ASCII-armored Key>	x		Key des Users	
END-OF-KEY		x		Schlüsselbegriff markiert Ende von KEY	
KEY-ID:	< KeyID>	x			au
USER-ID:	<USER-ID>	x			au

PRIME-USER-ID:	<USER-ID>	x		Erste UserID in Key	au
FINGERPRINT	< Fingerprint>	x			au
KEYSIZE	< Keylength >	x			au
KEYTYPE	< Key-Algo > < Hash-Algo. >	x		verwendete Algorithmem für Key und Hash	au
PGPVERSION	< Version >	x		PGP Version mit der Key generiert wurde	au
CREATION	< Tag-Monat-Jahr>	x		Erzeugungsdatum des Keys	au
EXPIRATION	< Tag-Monat-Jahr>	x		Verfallsdatum des Keys	au
USAGE	< Sign & Encrypt >	x		Verwendungszeck	au
CN	<Name>	x		Name des Benutzers;	x
SN	<Vorname>	x		Nachname des Benutzers	x
MAIL	<Mail-Adresse>	x		Mail-Adresse des Benutzers	x
DESCRIPTION	< Text>	x		Beschreibung	x
KEYOWNER	USER	x		Status des Schlüsseleigentümers	
	CA	x			
	RA	x			

CREATIONMODE:	OWN	x		Art der Schlüsselerzeugung	
	AUTO	x			
	CA	x			
	UNKNOWN	x			
CA-POLICY	<URL>	x	x	URL der Policy wenn User = CA / RA	
CA-DN	< DN der CA>	x	x	DN wenn Benutzer = CA / RA	
CA-CRLLINK	< URL>	x	x	URL der CA-CRL wenn User = CA	
REVCERT	YES	x		Revokation-Zertificat liegt vor	
	NO	x			
END-OF-KEYDEF		x	x	Schlüsselbegriff markiert das Ende des Datensatzes eines Users	