



Note:

Deprecation of a PKCS #11 key in LDAP should point to a replacing key, so that info should also be present.

Question to Rick:

What to do if there is no new key?
Simply dropping a key may be bad,
if it may still be used for decryption.

Better:

When not rolling the key for this
identity, better also remove it
from the localid.db